

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

JEHAN ZIBOUKH, MARGRET PHILIE,
VERA FIGLOCK, NICOLE MAY, TYANA
DAUGHTERY, SOLALIZ HERNANDEZ,
AND DEBRA KRYSTYN, on behalf of
themselves and all others similarly situated,

Plaintiffs,

v.

WHALECO INC. D/B/A TEMU, AND
PDD HOLDINGS INC. F/K/A
PINDUODUO INC.,

Defendants.

Case No. _____

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. PARTIES	6
A. Plaintiffs	6
1. Illinois Plaintiff	6
2. California Plaintiffs	6
3. Massachusetts Plaintiffs	7
4. Virginia Plaintiff	7
B. Defendants	7
1. PDD Holdings Inc. f/k/a Pinduoduo Inc.	7
2. Whaleco Inc. d/b/a Temu	8
C. Alter Ego and Single Enterprise Allegations.....	8
III. JURISDICTION AND VENUE	9
IV. BACKGROUND	11
A. Defendant PDD Holdings Inc. Is A Large, Tech-Based Business That Originated In China, Developing An Online Retail App Named Pinduoduo.....	11
B. PDD Holdings Inc. Recently Developed A Second Online Retail App, Temu, That Is Based On The Pinduoduo App and Which It Aggressively Marketed In The United States	12
C. Experts Have Concluded That Defendants’ Temu And Pinduoduo Apps Violate Users’ Data Privacy Rights In Multiple Ways	14
1. Temu Violates Users’ Data Privacy.....	15
2. Temu Is Designed To Hide Its Malicious Features	23
3. Temu Subjects User Data To Misappropriation By Chinese Authorities.	26
D. Defendants Are Violating Plaintiffs’ Right to Privacy Of Their Data	33

E.	Defendants Utilize Deceptive, Manipulative, And Unscrupulous Practices To Maximize Their Access To User Data	36
F.	Additional Allegations Concerning the Named Plaintiffs.....	43
V.	CLASS ALLEGATIONS	46
VI.	APPLICABLE LAW.....	51
VII.	COUNTS.....	52
	FIRST COUNT: Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.....	52
	SECOND COUNT: Violation of the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510 <i>et seq.</i>	53
	THIRD COUNT: Violation of the Right to Privacy Under Mass. Gen. Laws Ch. 214, § 1B.....	55
	FOURTH COUNT: Violation of the Massachusetts Wiretap Act, Mass. Gen. Laws, Ch. 272, § 99	59
	FIFTH COUNT: Restitution / Unjust Enrichment	62
	SIXTH COUNT: Violation of Illinois’s Biometric Information Privacy Act, 740 ILCS 14/1, <i>et seq.</i>	65
	SEVENTH COUNT: Violation of the California Comprehensive Data Access and Fraud Act, Cal. Pen. C. § 502.....	71
	EIGHTH COUNT: Violation of the Right of Privacy Under the California Constitution	72
	NINTH COUNT: Intrusion Upon Seclusion	75
	TENTH COUNT: Violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200 <i>et seq.</i>	78
	ELEVENTH COUNT: Violation of the California False Advertising Law, Bus. & Prof. C. §§ 17500 <i>et seq.</i>	81
	TWELFTH COUNT: Violation of the Virginia Computer Crimes Act, Va. Code § 18.2-152.1, <i>et seq.</i>	83
VIII.	REQUEST FOR RELIEF	86
IX.	DEMAND FOR JURY TRIAL	87

Plaintiffs, individually and on behalf of all others similarly situated (the “Class”), bring this class action complaint based upon personal knowledge of the facts pertaining to them and on information and belief based upon investigation of counsel as to all other matters, by and through undersigned counsel, against PDD Holdings Inc. f/k/a Pinduoduo Inc. and Whaleco Inc. d/b/a Temu (“Temu”) (collectively, “Defendants”).

I. INTRODUCTION

1. In 2022, Defendants launched an online shopping platform, Temu, in the United States. The Temu mobile app and website (the “Temu platform” or “Temu app”), allows users to purchase low-cost goods manufactured in China.

2. Temu is ultimately owned by the Nasdaq-listed Chinese company PDD Holdings Inc., which runs the Chinese e-commerce giant Pinduoduo, an online shopping platform that is the precursor for the Temu platform (the “Pinduoduo platform” or “Pinduoduo app”).

3. The Temu app has become extremely popular. The app was introduced in the United States last year and has been extensively promoted, including in a widely viewed Super Bowl commercial, using the tagline: “Shop like a billionaire.” Temu was the most downloaded app in the US for the last few months of 2022 and has remained there throughout 2023, achieving more than 100 million users in the United States by May 2023.¹ The Temu app is one of the most popular apps for mobile devices in the United States and the world.

4. However, this growth has a dark side which is the subject of this case. Experts who have reviewed the app have concluded that the “TEMU app is purposefully and intentionally loaded with tools to execute virulent and dangerous malware and spyware activities on user devices

¹ <https://www.businessofapps.com/data/temu-statistics/#:~:text=Like%20Wish%20and%20other%20discount,almost%20every%20day%20in%202023.>

which have downloaded and installed the TEMU app.”² In addition, they have concluded that “Temu misled people about how it uses their data.”³

5. According to these experts, Temu collects user data beyond what is necessary for an online shopping app, including biometric information and data from users of the app. Temu has “a complete arsenal of tools to exfiltrate virtually all the private data on a user’s device and perform nearly any malign action upon command trigger from a remote server.”⁴ Accordingly, it gains access to “literally everything on your phone.”⁵ This is particularly concerning, given that biometric information such as facial characteristics, voiceprints, and fingerprints are immutable characteristics that can be misused by unscrupulous actors.⁶

6. In addition, experts have concluded that the app collects a greater amount of information from users than is disclosed. Accordingly, users are not able to effectively consent to the collection of their data by the app, given that Defendants have misled users regarding the scope of the data collected from them and the ways in which their data is used.⁷ Experts have found that

² <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

³ <https://www.politico.eu/article/booming-chinese-shopping-app-temu-faces-western-scrutiny-over-data-security-2/>.

⁴ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

⁵ <https://www.komando.com/kims-column/temu-security-concerns/883861/>.

⁶ <https://www.compassitc.com/blog/temu-app-poses-potential-data-risk-for-consumers#:~:text=The%20U.S%20has%20accused%20Temu,vulnerabilities%20in%20Android%20operating%20systems.>

⁷ <https://www.politico.eu/article/booming-chinese-shopping-app-temu-faces-western-scrutiny-over-data-security-2/>.

Temu is particularly “dangerous” because it “bypasses’ phone security systems to read a user’s private messages, make changes to the phone’s settings and track notifications.”⁸

7. As a result of such privacy violations, it has been reported that Apple recently concluded that the Temu app “violated the company’s mandatory privacy rules.”⁹ Indeed, experts have found “smoking gun evidence” that the “widely downloaded shopping app TEMU is the most dangerous malware/spyware package currently in widespread circulation.”¹⁰

8. Moreover, experts have found that Defendants have gone to great lengths to conceal their privacy violations from Temu’s users so that Defendants may continue to steal their data. “It is evident that great efforts were taken to intentionally hide the malicious intent and intrusiveness of the software.”¹¹

9. These privacy violations are particularly concerning because Temu is a Chinese-owned company. As a result, the data collected by the Temu app is ultimately available to individuals and entities in China. Under Chinese law, in turn, such user data possessed by, controlled by, or accessible to individuals and entities in China may be demanded by the government at any time. The accessibility of user data to Chinese entities and ultimately the Chinese government is not adequately disclosed to users of the Temu app.

10. Such concerns regarding data privacy associated with Temu and other Chinese-owned apps have led government entities to ban or restrict their use. As with other Chinese-

⁸ <https://www.ibtimes.com/after-tiktok-montana-bans-wechat-temu-telegram-government-devices-3694060>.

⁹ <https://www.politico.eu/article/booming-chinese-shopping-app-temu-faces-western-scrutiny-over-data-security-2/>.

¹⁰ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

¹¹ *Id.*

owned apps, such as the TikTok app, Temu conveys “data to its Chinese parent company, [and] is legally unable to refuse to share data to the Chinese Government.”¹² Accordingly, the State of Montana recently banned the Temu app from government devices due to its significant concerns regarding the privacy of user data.¹³

11. These recent revelations regarding Temu’s data privacy violations are merely the latest in a string of privacy violations committed by the Defendants. As noted, the Temu app was a successor to the Pinduoduo online shopping app, which is owned by Temu’s parent company, Defendant PDD Holdings Inc. As with Temu, the Pinduoduo app has also been noted for its significant privacy violations. For example, the Pinduoduo app was recently suspended from the Google Play Store “due to the presence of malware on the Pinduoduo app that exploited vulnerabilities in Android operating systems.” According to reports, “Company insiders said the exploits were utilized to spy on users and competitors, allegedly to boost sales.”¹⁴ It has been reported that the same software engineers who developed the Pinduoduo app also worked on the Temu app.¹⁵

12. Defendants have sought to maximize their access to user data and their profits by implementing fundamentally unfair and deceptive trade practices. Defendants employ a variety of manipulative and deceptive business practices in an effort to get users to urge friends and

¹² See <https://inc.com/jason-aten/the-department-of-defense-is-warning-people-not-to-use-tiktok-over-national-security-concerns.html>.

¹³ <https://www.ibtimes.com/after-tiktok-montana-bans-wechat-temu-telegram-government-devices-3694060>.

¹⁴ <https://www.compassitc.com/blog/temu-app-poses-potential-data-risk-for-consumers#:~:text=The%20U.S%20has%20accused%20Temu,vulnerabilities%20in%20Android%20operating%20systems.>

¹⁵ <https://nypost.com/2023/08/05/why-the-chinese-shopping-app-is-a-scam/>.

acquaintances to sign up for the Temu app, thereby subjecting new users' data to unlawful collection by Defendants. For example, Temu users are bombarded with notifications seeking to entice them to refer new users in exchange for prizes and discounts. In addition, Temu targets and employs a network of paid influencers to lure new users to the platform. More generally, Defendants entice users to sign up for the Temu app with the promise of low-cost, high-quality goods. However, Defendants' representations are false. Goods sold on the Temu platform are frequently of low quality or counterfeit. In addition, as a congressional committee recently observed in a report on Chinese e-commerce, goods sold on Temu are frequently the product of forced labor extracted from the minority Uyghur population held in detention camps in the Xinjiang province in China. Through such deceptive and unfair practices, Defendants are able to reduce costs even further to expand the number of users who join the Temu platform and unwittingly give Defendants broad access to misappropriate their personal data. As a result, using the inducement of "that super low, too-good-to-be-true price on some gadget," Defendants trick users into giving them access to users' devices, and "TEMU is able to hack your phone from the moment you install the app, overriding the data privacy settings you think you have in place, as well as your intentions, helping itself to your contact list, your precise location, in some cases, control of your camera, screenshots of the apps running on your screen, and, depending on the permissions you may have given when you installed the app, your SMS text messages and other documents you may have on your phone."¹⁶

¹⁶ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

13. This is a proposed nationwide class action alleging violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 103; Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510 *et seq.*; the right to privacy under Mass. Gen. Laws Ch. 214, § 1B; the Massachusetts Wiretap Act, Mass. Gen. Laws, Ch. 272, § 99; and restitution/unjust enrichment. In addition, the complaint contains subclasses asserting additional state-law claims under Illinois, California and Virginia law, including claims under Illinois's Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*

II. PARTIES

A. Plaintiffs

1. Illinois Plaintiff

14. **Debra Krystyn** is a resident of Chicago, Illinois. She downloaded the Temu app and purchased products on the platform, thereby subjecting her personal and private data to misappropriation by Defendants.

2. California Plaintiffs

15. **Nicole May** is a resident of Santa Clarita, California. She downloaded the Temu app and purchased products on the platform, thereby subjecting her personal and private data to misappropriation by Defendants.

16. **Tyana Daugherty** is a resident of Los Angeles, California. She downloaded the Temu app, thereby subjecting her personal and private data to misappropriation by Defendants.

17. **Solaliz Hernandez** is a resident of Sylmar, California. She downloaded the Temu app, thereby subjecting her personal and private data to misappropriation by Defendants.

3. **Massachusetts Plaintiffs**

18. **Margret Philie** is a resident of Middleborough, Massachusetts. She downloaded the Temu app and purchased products on the platform, thereby subjecting her personal and private data to misappropriation by Defendants.

19. **Vera Figlock** is a resident of Taunton, Massachusetts. She downloaded the Temu app and purchased products on the platform, thereby subjecting her personal and private data to misappropriation by Defendants.

4. **Virginia Plaintiff**

20. **Jehan Ziboukh** is a resident of Richmond, Virginia, who initially downloaded and used the Temu app when she was a minor, thereby subjecting her personal and private data to misappropriation by Defendants.

B. **Defendants**

1. **PDD Holdings Inc. f/k/a Pinduoduo Inc.**

21. **Defendant PDD Holdings Inc.**, is a company that was founded in China in 2015 under the name Pinduoduo. It owns and operates a portfolio of businesses and is listed on the Nasdaq exchange in the United States. Among other things, PDD Holdings Inc., operates the Pinduoduo e-commerce platform that offers products in various categories, including agricultural produce, apparel, shoes, bags, mother and childcare products, food and beverage, electronic appliances, furniture and household goods, cosmetics and other personal care, sports and fitness items and auto accessories. It also owns the company that operates the Temu online marketplace. PDD Holdings Inc., was formerly known as Pinduoduo Inc., with headquarters in Shanghai, China. In February 2023, PDD Holdings Inc., moved its “principal executive offices” from

Shanghai, China to Dublin, Ireland.¹⁷ However, it continues to have significant operations in China, with multiple subsidiaries located within China. PDD Holdings Inc., is registered in the Cayman Islands.

2. Whaleco Inc. d/b/a Temu

22. Defendant Whaleco Inc., (“Temu”) is, and at all relevant times was, a corporation incorporated in Delaware and headquartered in Boston, Massachusetts. Temu is an online marketplace operated by the Chinese e-commerce company PDD Holdings Inc. It offers heavily discounted goods that are mostly shipped to consumers directly from China.

C. Alter Ego and Single Enterprise Allegations

23. Defendants do not function as separate and independent corporate entities. To the contrary, Defendant Temu is directly controlled by Defendant PDD Holdings Inc.

24. At all relevant times, Defendant PDD Holdings Inc., has directed the operations of Defendant Temu with respect to the Temu app, and Defendant Temu has reported to Defendant PDD Holdings Inc.

25. Moreover, employees from Defendant PDD Holdings Inc., performed work on the Temu app, including software engineers who previously developed the Pinduoduo app for PDD Holdings Inc.

26. Defendant PDD Holdings Inc., made key strategy decisions for Defendant Temu, which was charged with executing such decisions.

27. At all relevant times, and in connection with the matters alleged herein, each Defendant acted as an agent, servant, partner, joint venturer, and/or alter ego of the other

¹⁷ <https://www.cnbc.com/2023/05/04/chinas-pdd-holdings-parent-of-temu-moves-headquarters-to-ireland.html>.

Defendant, and acted in the course and proper scope of such agency, partnership, and relationship and/or in furtherance of such joint venture. Each Defendant acted with the knowledge and consent of the other Defendant and/or directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted and/or participated in the acts or transactions of the other Defendant.

28. At all relevant times, and in connection with the matters alleged herein, Defendants constituted a single enterprise with a unity of interest.

III. JURISDICTION AND VENUE

29. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) & 1367 because: (i) this is a class action in which the matter in controversy exceeds the sum of \$5,000,000, exclusive of interest and costs; (ii) there are 100 or more class members; and (iii) some members of the class are citizens of states different from some Defendants, and also because a Defendant is a citizens or subject of a foreign state.

30. This Court has personal jurisdiction over Defendants because: (i) they transact business in the United States, including in this District; (ii) they have substantial aggregate contacts with the United States, including in this District; and (iii) they engaged and are engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, including in this District, and they purposely availed themselves of the laws of the United States.

31. This Court further has personal jurisdiction with respect to the claims of the Illinois Subclass (defined below) because Defendants used and disseminated data derived directly from Illinois-based Temu users and exposed residents of Illinois to ongoing privacy risks within Illinois based on the collection, capture, obtainment, disclosure, redisclosure and dissemination of

their biometric identifiers and information. Furthermore, many of the images or other data Defendants used for their unlawful collection, capture and obtainment of biometric identifiers and information were created in Illinois, uploaded from Illinois, and/or managed via Illinois-based user accounts, computers, and mobile devices. Because of the scope and magnitude of Defendants' conduct, Defendants knew that their collection, capture, obtainment, disclosure, redisclosure and dissemination of impacted individuals' biometric identifiers and information would injure Illinois residents and citizens. Defendants knew or had reason to know that collecting, capturing, obtaining, disclosing, redisclosing and disseminating Illinois citizens' and residents' biometric identifiers and information without providing the requisite notice or obtaining the requisite releases would deprive Illinois citizens and residents of their statutorily-protected privacy rights, neutralize Illinois citizens' and residents' ability to control access to their biometric identifiers and information via their Illinois-managed devices and exposed minors and other in Illinois to potential surveillance and other privacy harms as they went about their lives within the state.

32. Furthermore, through the Temu app, Defendants actively collect information harvested from the Illinois-based devices of Illinois residents, including location information based on users' SIM cards and/or IP addresses.

33. Defendants use this harvested information to provide users with location-based services directed toward Illinois.

34. Defendants' deliberate gathering of Illinois users' personally identifiable information is intentionally targeted toward Illinois residents, including Plaintiffs and the Class, and constitutes purposeful activity directed at devices and individuals in Illinois.

35. In addition, Defendants transacted business in the State with Illinois residents and shipped merchandise into the state in exchange for payments made by Illinois residents.

36. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the acts or omissions giving rise to the claims alleged herein occurred in Illinois. Alternatively, venue is proper under 28 U.S.C. § 1391(b)(3) because this Court has personal jurisdiction over Defendants.

IV. BACKGROUND

A. Defendant PDD Holdings Inc. Is A Large, Tech-Based Business That Originated In China, Developing An Online Retail App Named Pinduoduo

37. Defendant PDD Holdings Inc. is a large tech conglomerate that was founded in 2015 by Chinese businessman and software engineer Colin Huang. It is one of China's largest companies with an estimated valuation of more than \$100 billion.¹⁸ In the last year alone, the conglomerate achieved a gross operating profit of more than \$4 billion.¹⁹ Its total revenue for the year was nearly \$19 billion.²⁰

38. PDD Holdings Inc. operates a series of subsidiaries in China and has long maintained its corporate headquarters in Shanghai, China. However, in an effort to obscure its connections to China, PDD Holdings Inc., recently disclosed that it was moving its "principal executive offices" to Dublin, Ireland. Nonetheless, the vast majority of PDD Holdings Inc.'s business operations, including several subsidiaries, continue to be located in China.

¹⁸ <https://www.wsj.com/market-data/quotes/PDD>.

¹⁹ <https://investor.pddholdings.com/news-releases/news-release-details/pdd-holdings-announces-fourth-quarter-2022-and-fiscal-year-2022>.

²⁰ *Id.*

39. Among other business activities, PDD Holdings Inc., operates Pinduoduo, an e-commerce platform created in China that offers products in various categories, including agricultural produce, apparel, shoes, bags, mother and childcare products, food and beverage, electronic appliances, furniture and household goods, cosmetics and other personal care, sports and fitness items and auto accessories.

40. Pinduoduo was developed in China to compete with Chinese online retailers Alibaba and JD.com by selling low-priced goods. The Pinduoduo app serves as a marketplace that recruits China-based suppliers to offer products and provides a range of low-cost products to consumers who visit its site.

B. PDD Holdings Inc. Recently Developed A Second Online Retail App, Temu, That Is Based On The Pinduoduo App and Which It Aggressively Marketed In The United States

41. Defendant PDD Holdings Inc., subsequently developed a second online retail app, the Temu app, that was based on the Pinduoduo app. Indeed, many of the same software engineers who developed Pinduoduo also worked on what became known as the Temu app.²¹ Nonetheless, as with PDD Holdings, Defendants have sought to obscure Temu's relationship to China (and to the precursor Pinduoduo app) by asserting publicly that "the Temu platform operates primarily in the United States."²²

42. Defendants made the Temu app available to consumers in the United States in September 2022. Since that time, Defendants have heavily promoted the Temu app, including through television advertisements, large online ad campaigns, and sponsorships. Temu's

²¹ <https://nypost.com/2023/08/05/why-the-chinese-shopping-app-is-a-scam/>.

²² PDD Holdings Inc. Annual Report (2022).

marketing budget for 2023 alone is reportedly more than \$7 billion; in contrast, Walmart's 2022 marketing budget was only \$3.9 billion.²³

43. Like the Pinduoduo app, the Temu app provides a marketplace for Chinese suppliers to offer their products. However, the Temu app also handles delivery, promotion and after-sales services for merchants on its platform. Temu's network now includes more than 80,000 suppliers.²⁴

44. Defendants market the Temu app as offering "affordable, quality products," claiming Temu sells "the best products globally,"²⁵ and they have positioned it to compete with online retail companies such as Amazon. Defendants market the app using the tagline "Shop Like a Billionaire" to communicate to consumers that the app provides significant value to consumers by providing them access to deeply discounted goods that are comparable in quality to higher-priced goods offered by other retailers.

45. Defendants have used a variety of mechanisms to aggressively market the app in the United States. Among other things, in February 2023, Temu ran an advertisement promoting the app during the Super Bowl. In addition to the initial and subsequent views of the advertisement

²³ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

²⁴ <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fast-fashion-and-the-uyghur-genocide-interim-findings.pdf>.

²⁵ https://www.temu.com/about-temu.html?_x_vst_scene=adg&_x_ads_sub_channel=search&_x_ads_channel=google&_x_ads_account=1213016319&_x_ads_set=19694142866&_x_ads_id=141345685810&_x_ads_creative_id=648389974220&_x_ns_source=g&_x_ns_gclid=EAIaIQobChMIp-qu7uHrgQMVzOHjBx3NbwnPEAAAYASAAEgJG7vD_BwE&_x_ns_placement=&_x_ns_match_type=e&_x_ns_ad_position=&_x_ns_product_id=&_x_ns_target=&_x_ns_devicemod=el=&_x_ns_wbraid=CjkKCQjwyY6pBhDkARlOAlxVarMMiImKANb_YPCex1QIQIP18Qo6VyWLbo5bKiA0ncz9-bGx8hoCReg&_x_ns_gbraid=0AAAAAo4mICFRpdCyS3-Cw22-MR1T_CF7V&_x_ns_keyword=temu&_x_ns_targetid=kwd-5681707004&refer_page_name=home&refer_page_id=10005_1696950675462_i3umf3qzlf&refer_page_sn=10005&_x_sessn_id=hbzdvdage0f.

on television, the ad has received more than 341 million views online on the YouTube app alone.²⁶

46. As a result of Defendants' heavy promotion of the Temu app, it has experienced exponential growth. It has become one of the most popular apps available in the United States, and already has more than 100 million active users.²⁷ As a result, the market capitalization of Defendant PDD Holdings has swelled to approximately \$135 billion.²⁸

47. Temu users purchase billions of dollars of goods on the Temu app, through millions of individual transactions. As a result, Temu is responsible for tens of millions of shipments that are sent to the United States each year through Temu's network of more than 80,000 China-based sellers participating in its online marketplace.²⁹

C. Experts Have Concluded That Defendants' Temu And Pinduoduo Apps Violate Users' Data Privacy Rights In Multiple Ways

48. Temu has been identified as one of the Chinese-affiliated apps that pose a significant threat to user data privacy. Experts in the field as well as government authorities have repeatedly noted the security risks associated with China-affiliated apps such as Tiktok and Temu, which violate users' data privacy rights in multiple ways. Such observations have led to restrictions of such Chinese apps and outright bans due to data privacy concerns.

²⁶ <https://www.latimes.com/business/story/2023-06-15/temu-sells-products-linked-to-forced-labor-in-china>.

²⁷ <https://www.businessofapps.com/data/temu-statistics/#:~:text=Like%20Wish%20and%20other%20discount,almost%20every%20day%20in%202023>.

²⁸ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

²⁹ <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fast-fashion-and-the-uyghur-genocide-interim-findings.pdf>.

1. Temu Violates Users' Data Privacy.

49. Analysts have concluded that Temu specifically is using the inducement of low-cost Chinese-made goods to lure users into unknowingly providing unwarranted and broad-ranging access to their private data in ways that are deceptive.

50. Such concerns began to emerge after Temu's precursor, the Pinduoduo app, was pulled from Google's Play Store due to the presence of malware on the app that exploited vulnerabilities in Android operating systems. According to one report, "Company insiders said the exploits were utilized to spy on users and competitors, allegedly to boost sales. Pinduoduo requested as many as 83 permissions, including access to biometrics, Bluetooth, and Wi-Fi network information. Temu is not as aggressive in its data requests as Pinduoduo, although the fact that Temu requests 24 permissions, including access to Bluetooth and Wi-Fi network information, is a cause for concern. These permissions might seem innocuous at first glance, but cybersecurity experts argue there is no need for an e-commerce app to store biometric data, and any request to do so should be treated with suspicion. Unlike passwords, biometric data like fingerprints cannot be changed, which makes them a lucrative target for cybercriminals."³⁰

51. Analysts, including experts at Google, concluded that the Pinduoduo app was covertly collecting private and personal data from users without their knowledge and consent, including highly sensitive biometric data contained on users' devices. These functions were not accidental—they were intentionally built into the design of the app: "Pinduoduo's malware was not a fringe or circumstantial effort. PDD recruited and hired a team of 100 programmers to find and

³⁰ <https://www.compassitc.com/blog/temu-app-poses-potential-data-risk-for-consumers#:~:text=The%20U.S%20has%20accused%20Temu,vulnerabilities%20in%20Android%20operating%20systems.>

exploit OEM customizations of Android (installed on mainstream brands of low-priced smartphones), intending to exploit vulnerabilities audited less often than the mainline Android codebase (estimates of over 50 such vulnerabilities were targeted).”³¹

52. Moreover, even after Defendants made changes to the Pinduoduo app in response to the suspension, it continued to violate users’ privacy rights. For example, multiple security vendors continue to rate Pinduoduo as “malicious”, as reported by the malware statistics service VirusTotal.com.

53. Analysts further concluded that Pinduoduo’s data privacy policies and practices were deceptive and that many of the features of the Pinduoduo app that were problematic were shared with the Temu app. Indeed, it has been reported that Apple recently expressed similar concerns regarding the Temu app, concluding that the app did not comply with Apple’s data privacy standards and that Temu was misleading users regarding how their data is being used. As one report noted: “Apple said Temu previously violated the company’s mandatory privacy rules. It said it had found that Temu misled people about how it uses their data. Temu’s so-called privacy nutrition labels – descriptions about the types of data an app can access, how it does so and what it uses them for – did not accurately reflect its privacy policy, said Apple. Temu also isn’t letting users choose not to be tracked on the internet.”³²

54. Such concerns have also been expressed recently by government authorities who have examined the app. For example, the State of Montana recently banned the Temu app on

³¹ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

³² <https://www.politico.eu/article/booming-chinese-shopping-app-temu-faces-western-scrutiny-over-data-security-2/>.

government devices, along with other Chinese apps that have engaged in data privacy violations, such as TikTok.³³ As the State's Chief Information Officer noted when the action was announced, it was implemented to ban apps that pose a "risk of foreign adversaries obtaining Montanans' personal, private, sensitive information and data" from government-issued devices.³⁴ Similarly, in April 2023, the U.S.-China Economic and Security Review Commission, a government entity established by Congress to investigate, assess, and report annually on the national security implications of the economic relationship between the United States and the People's Republic of China, issued a report noting the significant data risks associated specifically with the Temu app.³⁵

55. Subsequent technical analyses have concluded that the Temu app is "even more 'malicious' than the suspended pinduoduo-649-0 app."³⁶ As analysts have observed, the scope of the data collected by Temu is sweeping and goes well beyond the scope of the data that is needed to run an online shopping app. As one commentator noted, in addition to Bluetooth and Wi-Fi access, "Temu gains full access to all your contacts, calendars, and photo albums, plus all your social media accounts, chats, and texts. In other words, literally everything on your phone.... No shopping app needs this much control, especially one tied to Communist China."³⁷ As another commentator observed in commenting on the Montana ban, "Temu is dangerous," said tech

³³ <https://www.ibtimes.com/after-tiktok-montana-bans-wechat-temu-telegram-government-devices-3694060>.

³⁴ *Id.*

³⁵ <https://www.uscc.gov/research/shein-temu-and-chinese-e-commerce-data-risks-sourcing-violations-and-trade-loopholes>.

³⁶ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

³⁷ <https://www.komando.com/kims-column/temu-security-concerns/883861/>.

writer Albert Khoury,' warning that the app 'bypasses' phone security systems to read a user's private messages, make changes to the phone's settings and track notifications."³⁸

56. One technical investigation of the app published by an analyst firm on September 6, 2023, concluded that the "TEMU app is purposefully and intentionally loaded with tools to execute virulent and dangerous malware and spyware activities on user devices which have downloaded and installed the TEMU app."³⁹ The analysis went so far as to claim that Defendant PDD Holdings was a "fraudulent company" and that "its shopping app TEMU is cleverly hidden spyware that poses an urgent security threat to U.S. national interests."⁴⁰ Indeed, the analysis purported to provide "smoking gun evidence" that the "widely downloaded shopping app TEMU is the most dangerous malware/spyware package currently in widespread circulation."⁴¹

57. Among the primary findings of the report were the following:

- a. "The app has hidden functions that allow for extensive data exfiltration unbeknown to users, potentially giving bad actors full access to almost all data on customers' mobile devices."
- b. "It is evident that great efforts were taken to intentionally hide the malicious intent and intrusiveness of the software."

³⁸ <https://www.ibtimes.com/after-tiktok-montana-bans-wechat-temu-telegram-government-devices-3694060>.

³⁹ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

⁴⁰ *Id.*

⁴¹ *Id.*

- c. “We engaged numerous independent data security experts to decompile and analyze TEMU app’s code, integrated with experts of our own staff, and analysts who have written independently in the public domain.”
- d. “Contributing to the danger of mass data exfiltration is the fast uptake rate of the TEMU app: over 100 million app downloads in the last 9 months, all in U.S. and Europe. TEMU is not offered in China.”
- e. “The TEMU app development team includes 100 engineers who built the Pinduoduo app, which earned a suspension from the Google Play Store.”
- f. “Pinduoduo app got reinstated by removing the ‘bad parts,’ some of which were identically utilized as components of the TEMU app, strongly indicating malicious intent.”
- g. “We strongly suspect that TEMU is already, or intends to, illegally sell stolen data from Western country customers to sustain a business model that is otherwise doomed for failure.”⁴²

58. Specifically, the analysis concluded that the Temu app contains malware, spyware, and other means to “plunder” user data: “TEMU has laid an extensive software foundation to recklessly plunder its customers’ data. Our staff analysis, verified by numerous expert confirmations, both proprietary experts we hired, plus those independently published in the public domain, find malware, spyware, and several levels of exceptionally threatening software behavior.”⁴³

⁴² *Id.*

⁴³ *Id.*

59. The analysis further found that the Temu app has the capability to hack users' phones and override data privacy settings that users have purposely set to prevent their data from being accessed: "So in exchange for that super low, too-good-to-be-true price on some gadget, we warn you that TEMU is able to hack your phone from the moment you install the app, overriding the data privacy settings you think you have in place, as well as your intentions, helping itself to your contact list, your precise location, in some cases, control of your camera, screenshots of the apps running on your screen, and, depending on the permissions you may have given when you installed the app, your SMS text messages and other documents you may have on your phone."⁴⁴

60. Technical analysis of the Temu app found "all the signs of red-flag concern," noting that "[t]he calls to outside device data and functions that violate users' privacy are far more aggressive than any well-known consumer shopping app." As depicted in the chart below, the analysis found "a stack of software functions that are completely inappropriate to and dangerous in this type of software"⁴⁵:

Security issue	TEMU	SHEIN	Alibaba.com	Amazon	TikTok	eBay
1 Local compiling with "package compile" executed with <code>getRuntime.exec()</code>	Yes	No	No	No	No	No
2 Requesting information if app runs with root rights ("superuser")	Yes	Yes	Yes	Yes	No	Yes
3 Request process list with " <code>getRunningAppProcesses()</code> "	Yes	Yes	Yes	Yes	Yes	Yes
4 Requesting system logs from <code>"/system/bin/logcat"</code>	Yes	No	No	No	No	No
5 Accessing debugger status with " <code>Debug.isDebuggerConnected()</code> "	Yes	Yes	Yes	Yes	No	Yes
6 Reading and writing system files in <code>"/sys/devices/"</code>	Yes	Yes	Yes	Yes	Yes	No
7 Accessing external storage with <code>"ExternalStorage"</code>	Yes	Yes	Yes	Yes	Yes	Yes
8 Making screenshots (" <code>getRootView()</code> ", " <code>peekDecorView()</code> " in " <code>getWindow()</code> ")	Yes	Yes	Yes	Yes	Yes	No
9 Requesting the MAC address	Yes	Yes	Yes	Yes	No	Yes
10 Putting MAC address into a JSON to send the information to server	Yes	No	No	No	No	No
11 Code obfuscation with most JAVA code: unnamed files, folders, functions	Yes	No	No	No	Yes	No
12 android.permission.CAMERA	Yes	Yes	Yes	Yes	Yes	Yes
13 android.permission.WRITE_EXTERNAL_STORAGE	Yes	Yes	Yes	Yes	Yes	Yes
14 android.permission.RECORD_AUDIO	Yes	No	Yes	Yes	Yes	No
15 android.permission.INSTALL_PACKAGES	Yes	No	No	No	No	No
16 android.permission.INTERNET	Yes	No	Yes	Yes	No	No
17 android.permission.WAKE_LOCK	Yes	No	Yes	No	No	No
18 Putting location information into JSON to send the information to server	Yes	No	No	Yes	No	No

⁴⁴ *Id.*

⁴⁵ *Id.*

61. For example, the “TEMU app is referencing systems data outside the bounds of TEMU’s own app. TEMU seemingly reads the user’s system logs. This gives TEMU the ability to track user actions with other apps running on the user’s device.”⁴⁶

62. The app also collects identifying information unique to a user’s device. Specifically, “TEMU asks for the MAC address, and other device information, and inserts it into a JSON object to be sent to the server. This is especially aggressive. Why does a shopping app need a database of technical details of their customers’ devices?”⁴⁷

63. The Temu app also has the capability to take screenshots of user phones and store those to a file, which can be another way to “spy on customers’ activities” with respect to other programs and data. Again, there is no legitimate reason for a function like this, given that Temu is a shopping app.⁴⁸

64. Temu also has the ability to read and transmit files on the user’s system “with little or no encryption.” Again, there is no legitimate reason that a shopping app would seek to intentionally lower encryption standards for its users.⁴⁹

65. Temu can access users’ cameras and microphones whenever the app is running. While users can upload photos using the Temu app, there is no reason that a shopping app would require the unrestricted ability to control users’ cameras and microphones at all times. Moreover,

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ *Id.*

such a function provides another means by which the Temu app can surreptitiously collect user biometric data and information such as video, facial image, and voiceprint data.⁵⁰

66. Temu is particularly malicious because much of the data collection occurs as soon as the app is downloaded. As reported in a recent technical report: “TEMU sends a lot of detailed user and system data elements as soon as the app is loaded.’ The user’s system gets queried in detail, so all that information is available to send to TEMU servers. (As noted above, this includes the device’s unique MAC address.) No user permission is required to gather any of this category of information.” Temu contains “a complete arsenal of tools to exfiltrate virtually all the private data on a user’s device and perform nearly any malign action upon command trigger from a remote server.”⁵¹

67. As one analyst observed, the immediate broad-based collection of such data violates user privacy: “I intercepted http traffic sent by the app, the first anomaly I noticed was the amount of data being sent as soon as you launch the app. This system information should not be disclosed, this is a clear violation of the user’s privacy. And I really don’t see what a ‘shopping’ app would do with the user’s operating processes.... Let alone his phone’s serial number.”⁵²

68. In addition to the unauthorized collection of their data, users may suffer additional injuries; the data collected from Temu users by these unauthorized means can be misused by Defendants themselves in ways that are not authorized, and as analysts have observed, may be sold or given to unauthorized third parties without the consent of Temu users. Indeed, as analysts have noted, regardless of whether users authorized the initial collection of such data by Defendants,

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Id.*

Temu users may be subjected to additional injuries, including the provision or sale of their data to unauthorized third parties or the use of their data in ways that users did not authorize by Defendants themselves.

2. Temu Is Designed To Hide Its Malicious Features

69. Further, experts who have examined the Temu app in detail have concluded that it is purposefully designed to hide these malicious features and that Defendants have taken actions to prevent users from discovering the app's numerous data privacy violations. A recent technical analysis found "clues in the software that reflect the app engineers' strong intention to purposefully cloak and obscure what the app actually performs when it is executing."⁵³

70. The Temu app contains technology (encrypt, decrypt or shift integer signals) that obscures the source code and system calls so that intrusive and dangerous calls are harder to detect when an app store or others perform security scans. In addition, the Temu app contains a `runtime.exec()` function that allows Temu to get compiled code onto the user's system at runtime that has not been seen by any security detection scans. These features alone demonstrate that the Temu app is purposefully designed to be "very virulent malware/spyware."⁵⁴

71. In addition, technical analysis of the app has uncovered that many of the "red-flag" issues uncovered with the app "occur in parts of the code that are proprietary, obscured, and/or from a code library rarely used, poorly programmed by a niche company." This is inconsistent with common practice and appears designed to obscure the dangerous features of the app so that

⁵³ *Id.*

⁵⁴ *Id.*

they will not be disclosed to the public and will avoid scrutiny by the app stores that provide the app to the public.⁵⁵

72. Thus, for example, a technical analysis found a “package compile” function that was “not visible to security scans before or during installation of the app, or even with elaborate penetration testing.” As a result, “TEMU’s app could have passed all the tests for approval into Google’s Play Store, despite having an open door built in for an unbounded use of exploitative methods.” “Put another way, if all the rest of the objectionable code was removed, while this one backdoor went undetected due to its concealment, the app could become just as malignant, by changing its behavior, controlled by foreign servers, in almost all possible ways and reactive to all future developments of the app, the regulations and all other possible influences.”⁵⁶

73. In addition, the Temu app seeks to obscure the permissions that are given to the app to access information on users’ phones. “[M]any of these permissions in TEMU’s source code are not listed in their Android Manifest file, which is the standardized overview source for an app.” In addition, the Temu app deceptively requests permissions in ways that do not clearly inform users that they are providing certain permissions to the app. Accordingly, because the Temu app “masks its intentions” by using such deceptive means, “You wouldn’t suspect that the TEMU app contains a full stack of malware/spyware tools to do just about anything it wants with your phone and get nearly anything stored on it sent to its own servers in the background.”⁵⁷

74. The Temu app also contains functions to alert the app if a debugger is engaged. Such a feature is likely incorporated into the app “to obstruct or obscure analysis of the app, and

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *Id.*

most likely to change app behavior if an analyst is inspecting it dynamically.” As one expert noted, this is a “HUGE red flag” because “Detecting a debugger means ... you don’t want anyone else to know what code you’re running.”⁵⁸

75. The files, folders, classes, and functions of the Temu app are also designed, named, and cross-reference each other in a highly complex way that is designed to hamper investigation of the malicious aspects of the app. Indeed, analysts have concluded that “it is practically impossible for a human to read the decompiled code, and we believe TEMU uses additional tools in the compiling process to create this obfuscation. The most outstanding indicator of TEMU’s code obfuscation is the top-level view of the JAVA source code after decompiling.” These practices are in contrast to other apps that are much more transparent.⁵⁹

76. In addition, Defendants have sought to cover their tracks by removing from the public domain prior versions of files associated with the app and have deleted features of the app when necessary to avoid detection of their wrongdoing. Among other things, analysts have concluded that “TEMU is hiding something” because of the following deceptive practices: 1) features of the Temu app that were similar to those of the Pinduoduo app were mysteriously deleted in May 2023 after Google suspended Pinduoduo for malicious spyware and 2) prior versions of certain files associated with the app have been removed from Google’s Play Store.⁶⁰

77. As one technical report noted with respect to the latter issue, “Many websites archive APK’s published in Google’s Play Store. However, TEMU’s app seems to have disappeared from many of these archives, in particular almost all with Google Page Rank 6 or higher that

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ *Id.*

appear on the top of Google searches. The TEMU APKs are removed from all websites with U.S. jurisdiction, indicating that legal measures by TEMU could be behind the exclusion from the web archives. Inaccessibility of the APK files makes malware research more cumbersome.”⁶¹

78. As reflected in the chart below, this lack of visibility with respect to Temu is in contrast to other apps.⁶²

APK Posting Website	Jurisdiction	Page Rank	Monthly traffic	TEMU	Shein	Amazon	Ebay	Ali-baba	TikTok
APKMirror.com	US	7	17.0M	no	yes	yes	yes	yes	yes
uptodown.com	ES	8	66.9M	no	yes	yes	yes	yes	yes
apkpure.com	US	8	64.2M	no*	yes	yes	yes	yes	yes
apkcombo.com	US	5	24.8M	no	yes	yes	yes	yes	yes
aptoide.com	PT	8	11.9	yes	yes	yes	yes	yes	yes
apk-dl.com	US	6	1.2M	no	no	yes	yes	yes	yes
apkmonk.com	US	6	3.3M	no	yes	yes	yes	yes	yes
apkbe.com	??	4	1.5M	yes**	yes	yes	yes	yes	yes
softpedia.com	RO	8	0.3M	no	no	yes	yes	yes	yes
appsapk.com	IL	6	0.2M	no	yes	yes	yes	no	yes
download.cnet.com	US	8	6.3M	no	yes	yes	yes	yes	yes
softonic.com	ES	8	43.0M	yes	yes	yes	yes	yes	yes
malavida.com	ES	8	13.4M	yes	yes	yes	yes	yes	yes
apkmody.io	SG	5	26.2M	yes	yes	yes	yes	yes	yes
alofapps.com	HK	2	2.1M	yes	yes	yes	yes	yes	yes

3. Temu Subjects User Data To Misappropriation By Chinese Authorities.

79. The data privacy violations documented with the Temu app are particularly concerning not only because they subject user data to unauthorized collection and potential sale to

⁶¹ *Id.*

⁶² *Id.*

third parties, but also because Temu's parent is a China-based company that is subject to Chinese law that requires companies to provide user data to the government upon request. As a technical analysis of the Temu app has noted, "Your personal data – much more than you ever assumed – is resold indiscriminately for marketing purposes, and in all probability available to Chinese Security authorities for data mining purposes. Chinese Government security agents or their AI computers might be looking at what products you or your family buy on TEMU as a source of leverage, influence, manipulation, 'cross-border remote justice', surveillance, or more."⁶³

80. As experts and government authorities have repeatedly observed, under applicable law, user data owned by Chinese companies is available on command to officials of the Chinese communist government. The Chinese government's ongoing efforts to acquire such private user data from American citizens—both legally and illegally—are well documented.

81. In October 2019, for example, United States Senators Charles Schumer and Tom Cotton sent a bipartisan letter to the Acting Director of National Intelligence describing risks associated with Chinese ownership of the TikTok app. The Senators noted that there was a significant security risk even though TikTok maintained that it "does not operate in China and stores U.S. user data in the U.S.," given that it was still "required to adhere to the laws of China." As the Senators explained, "Security experts have voiced concerns that China's vague patchwork of intelligence, national security, and cybersecurity laws compel Chinese companies to support and cooperate with intelligence work controlled by the Chinese Communist Party."⁶⁴

⁶³ *Id.*

⁶⁴ <https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-threats>; https://www.cotton.senate.gov/?p=press_release&id=1239.

82. A November 15, 2020, CBS News 60 Minutes broadcast addressed the dangers inherent in Chinese ownership of companies collecting American users' private and personally identifiable information. During the broadcast, among other things, a former member of the U.S. intelligence community observed that what makes the possession of U.S. user data by China-affiliated companies "particularly concerning" is that "[t]he Chinese have fused their government and their industry together so that they cooperate to achieve the ends of the state." As Senator Hawley observed during the broadcast, for example, the Chinese-owned parent company of TikTok had an express legal obligation to share such private user data with the Chinese government: "under Chinese law, TikTok, ByteDance, the parent, is required to share data with the Chinese Communist Party"; "all it takes is one knock on the door of their parent company, based in China, from a Communist Party official for that data to be transferred to the Chinese government's hands, whenever they need it."⁶⁵

83. In testimony given to Congress in November 2022, FBI Director Christopher Wray reiterated these concerns, noting that Chinese law requires Chinese companies to "do whatever the government wants them to in terms of sharing information or serving as a tool of the Chinese government." "And so that's plenty of reason by itself to be extremely concerned."⁶⁶

84. Based on such concerns, Senator Marco Rubio and Representative Mike Gallagher recently introduced legislation to completely ban TikTok "and other social media companies that are effectively controlled by the CCP [Communist Chinese Party] from operating in the United

⁶⁵ <https://www.nbcnews.com/politics/congress/hawley-takes-aim-tiktok-china-congressional-hearing-n1076586>.

⁶⁶ <https://www.npr.org/2022/11/17/1137155540/fbi-tiktok-national-security-concerns-china>.

States.”⁶⁷ There have been similar calls for specific action against Temu by commentators who argue that “TEMU is demonstrably more dangerous than TikTok. The app should be removed from the Google and Apple app stores.”⁶⁸

85. The Chinese government has sought to collect vast amounts of user data, including biometric data, in order to develop its artificial intelligence technologies. As the South China Morning Post reported: “China’s goal of becoming a global leader in artificial intelligence (AI) is nowhere more manifested than in how facial recognition technology has become a part of daily life in the world’s second-largest economy. Facial recognition systems, which are biometric computer applications that automatically identify an individual from a database of digital images, are now being used extensively in areas such as public security, financial services, transport and retail across the country.”⁶⁹ In fact, the Chinese government employs a variety of biometrics for population surveillance and control: “In addition to voice recognition, there are facial and pupil recognition, gathering of DNA samples—building the world’s largest DNA database—and fingerprint scans.”⁷⁰

86. Artificial intelligence algorithms feed on data to learn and improve – thus, the more data, the better the development of the algorithms driving the advance of the artificial

⁶⁷ <https://www.npr.org/2022/11/17/1137155540/fbi-tiktok-national-security-concerns-china>; see also <https://www.washingtonpost.com/opinions/2022/11/10/marco-rubio-ban-tiktok-america-china-mike-gallagher/>.

⁶⁸ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

⁶⁹ <https://www.scmp.com/tech/start-ups/article/2133234/meet-five-chinese-start-ups-pushing-facial-recognition-technology>.

⁷⁰ <https://brandscovery.com/business/content-2254742-china-gathers-peoples-voices-new-identification-technology-drawing-concerns>.

intelligence.⁷¹ With better artificial intelligence comes more effective population surveillance and control.

87. To advance these interrelated goals, the Chinese government has worked hand in glove with China-based technology companies to accumulate and share data. For example, the China-based company Megvii, a leader in computer vision, has the world's largest open-source database (Face++) for training other facial recognition algorithms. It has reportedly used government data banks to help compile this training program.⁷² Similarly, the Chinese government partnered with the China-based technology firm d-Ear Technologies to build a database of voiceprints for voice recognition purposes.⁷³

88. "Private [China-based] corporations and the [Chinese] Communist Party's security apparatus have grown together, discovering how the same data sets can both cater to consumers and help commissars calibrate repression. ... Many [China-based] tech firms make a point of hiring the relatives of high party officials, and a vast state database of headshots might be shared with a private firm to train new facial recognition software, while the firm's trove of real-time user data might be offered to police, for a panoramic view of potential 'troublemakers.'"⁷⁴

89. Such data gathering is not confined to China's borders. The Chinese government is compiling a tremendous storehouse of private and personally identifiable data on ordinary Americans. For example, Chinese government-sponsored hackers stole data belonging to

⁷¹ <https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/>.

⁷² *Id.*

⁷³ <https://brandscovery.com/business/content-2254742-china-gathers-people-s-voices-new-identification-technology-drawing-concerns>.

⁷⁴ <https://www.nytimes.com/interactive/2019/05/02/opinion/will-china-export-its-illiberal-innovation.html>.

approximately 500 million Marriott International guests. “[M]achine learning is yielding uses for large data sets that humans alone could not imagine – or even understand – given that machine learning can generate correlations among data that the machine itself can’t explain. ... Beijing’s plan may be simply to vacuum up as much data like this as possible and then see what today’s machine learning—or, better yet, tomorrow’s machine learning—can do with it.”⁷⁵

90. The lengths to which the Chinese government will go to obtain such data about ordinary Americans is further evidenced by other large-scale hacking schemes, including one involving 145 million Americans whose data was held by Equifax,⁷⁶ and another involving 78 million Americans whose data was held by Anthem.⁷⁷ “The United States assessed that China was building a vast database of who worked with whom in national security jobs, where they traveled and what their health histories were, according to American officials. Over time, China can use the data sets to improve its artificial intelligence capabilities to the point where it can predict which Americans will be primed for future grooming and recruitment”⁷⁸ “The hacks, security researchers said, were an extension of China’s evolving algorithmic surveillance system, which has greatly expanded over the past few years.”⁷⁹ Frequently, Chinese-based hacking against the U.S. has been tied specifically to the Chinese military.⁸⁰

⁷⁵ <https://www.justsecurity.org/62187/weapons-mass-consumerism-china-personal-information/>.

⁷⁶ <https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html>.

⁷⁷ <https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html>.

⁷⁸ <https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html>.

⁷⁹ <https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html>.

⁸⁰ <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>.

91. However, where, as here, Chinese-owned technology companies, like Defendants, have surreptitiously amassed such data on their own, there is no need for the Chinese government to engage in hacking to obtain the data. Under Chinese law, it is directly available to them.

92. That is because such China-based companies are required by law to secretly provide that data to the government upon demand:

The message contained in each of China's state security laws passed since the beginning of 2014 is clear: everyone is responsible for the party-state's security. According to the CCP's definition of state security, the Party's political leadership is central. ... And the party expects Chinese people and citizens to assist in collecting intelligence. The Intelligence Law states "any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of..." Not only is everyone required to participate in intelligence work when asked, but that participation must be kept secret.⁸¹

93. Chinese law requires Chinese citizens, and individuals and organizations or entities in China, to cooperate with "national intelligence work." It grants Chinese government and Communist Party officials broad, invasive authority to, among other things, access private networks, communications systems, and facilities to conduct inspections and reviews. These laws are broad and open-ended. Laws including, but not limited to, the National Security Law, Cybersecurity Law, and National Intelligence Law are part of "an interrelated package of national security, cyberspace, and law enforcement legislation" that "are aimed at strengthening the legal

⁸¹ <https://capx.co/britain-must-avoid-being-sucked-into-huaweis-moral-vacuum/>. See also <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense>.

basis for China's security activities and requiring Chinese and foreign citizens, enterprises, and organizations to cooperate with them."⁸²

94. The concerns with transferring personal data from U.S. users to Chinese-based companies such as TikTok and Temu are so great that Congress has drafted legislation that would prohibit the transfer of personal data from users in the United States to entities or individuals that are under the control or influence of China such as China-affiliated businesses like TikTok and Temu.⁸³

D. Defendants Are Violating Plaintiffs' Right to Privacy Of Their Data

95. As a result of their multiple violations of users' data privacy, Defendants possess identifying information, biometric identifiers and information, and other data sufficient to create a file of private and personally identifiable data and content for Temu users. Such files can be supplemented over time with additional private and personally identifiable user data and content, and all of this private and personally identifiable data and information has been, is, and will be used in the past, the present, and the future for economic and financial gain.

96. Meanwhile, Plaintiffs, the Class and the Subclasses have incurred, and continue to incur, harm as a result of the invasion of privacy stemming from Defendants' possession of their private and personally identifiable data and content – including their user identifiers, biometric identifiers and information, and other data.

⁸² M. Scot Tanner, Beijing's New National Intelligence Law: From Defense to Offense, LAWFARE (July 20, 2017), <https://bit.ly/3fXfB4A>.

⁸³ <https://www.congress.gov/bill/118th-congress/house-bill/1153/text>.

97. Plaintiffs, the Class and the Subclasses also have suffered and continue to suffer harm in the form of diminution of the value of their private and personally identifiable data and content as a result of Defendants' surreptitious and unlawful activities.

98. Plaintiffs, the Class, and the Subclasses have a reasonable expectation of privacy in the private and personally identifiable data and content on their mobile devices.

99. The United States Supreme Court has recognized that, in contemporary society, cell phones are so ubiquitous and inextricably intertwined with the user's personal privacy that the devices have become "almost a 'feature of human anatomy.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). The United States Constitution thus provides a privacy right that protects individuals against unreasonable governmental searches of their physical movements through historical cell phone records in the possession of their service providers. *Id.* at 2218.

100. As discussed above, Defendants have designed the Temu app to surreptitiously collect a wide range of data from Temu users. In addition, Defendants continue to take actions and have purposefully designed the Temu app to obscure and hide their unlawful collection of users' data.

101. Many of the categories of data and information collected by Defendants are particularly sensitive. For example, in addition to highly sensitive biometric information discussed below, Defendants also collect physical and digital location tracking data that is highly invasive of Temu users' privacy rights. "Location data is among the most sensitive personal information that a user can share with a company . . . Today, modern smartphones can reveal location data beyond a mere street address. The technology is sophisticated enough to identify on which floor of a

building the device is located.”⁸⁴ Over time, location data reveals private living patterns of Temu users, including where they work, where they reside, where they go to school, and when they are at each of these locations. Location data, either standing alone, or combined with other information, exposes deeply private and personal information about Temu users’ health, religion, politics and intimate relationships.

102. Moreover, as analysts have noted, there is no legitimate reason that a shopping app would be collecting such location data. The fact that location data is collected by Temu constitutes additional evidence that Defendants are selling users’ data to generate additional, covert profits: “Things like location data to me definitely raises a flag for me because I am not envisioning a lot of legitimate uses for it. And I know that selling location data is a big side business.”⁸⁵

103. More generally, the various functions and aspects of the Temu app described above make clear that it is an extremely malicious app designed to covertly harvest user data in violation of their privacy rights. As one technical analysis concluded:

TEMU has laid an extensive software foundation to recklessly plunder its customers’ data. Our staff analysis, verified by numerous expert confirmations, both proprietary experts we hired, plus those independently published in the public domain, find malware, spyware, and several levels of exceptionally threatening software behavior. So in exchange for that super low, too-good-to-be true price on some gadget, we warn you that TEMU is able to hack your phone from the moment you install the app, overriding the data privacy settings you think you have in place, as well as your intentions, helping itself to your contact list, your precise location, in some cases, control of your camera, screenshots of the apps

⁸⁴ <https://www.law360.com/consumerprotection/articles/1221312/sens-prod-zuckerberg-why-keep-tracking-user-locations->.

⁸⁵ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

running on your screen, and, depending on the permissions you may have given when you installed the app, your SMS text messages, and other documents you may have on your phone. Further, the TEMU app is engineered to hide its intentions and cloak detection of its invasive capabilities.⁸⁶

E. Defendants Utilize Deceptive, Manipulative, And Unscrupulous Practices To Maximize Their Access To User Data

104. Defendants actively utilize manipulative and deceptive practices in order to maximize the number of users who sign up to use the app, thereby maximizing the amount of data that Defendants can misappropriate. According to one commentator, “TEMU is a notoriously bad actor in its industry. We see rampant user manipulation, chain-letter-like affinity scams to drive signups, and overall, the most aggressive and questionable techniques to manipulate large numbers of people to install the app.”⁸⁷

105. Defendants seek to induce users to sign up for the Temu app with the promise of low-cost, high-quality goods manufactured in China. Defendants underscore this aspect of the platform through a variety of mechanisms such as pop-ups with wheels to spin for discounts, tokens to collect, and countdown clocks.



⁸⁶ *Id.*

⁸⁷ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

106. These tactics have been wildly successful: “PDD’s TEMU online marketplace is being reported as among the fastest uptaken apps in history.”⁸⁸

107. However, Defendants’ representations regarding the products sold on the Temu platform are false and serve only to further conceal its scheme to maximize the number of users who sign up to the platform and unwittingly subject their private data to theft by Defendants. For example, while Temu represents that it sells “affordable, quality products,” and indeed “the best products globally,”⁸⁹ there have been many complaints regarding the quality of goods sold on the site as well as the service provided by Temu. The Better Business Bureau alone has received hundreds of complaints in the past year, earning Temu a rating of 2.1 out of 5 stars.⁹⁰ Users experience undelivered packages and poor customer service. Moreover, even when goods are delivered, they are often of low quality, contrary to Temu’s marketing and representations.

108. For example, one analysis observed that “TEMU products as shipped often do not resemble the photos.”⁹¹ Users frequently receive low-quality, cheaply-made merchandise when the photo on the app indicates that they would receive high-quality goods. Moreover, photos and product descriptions are sometimes simply copied directly from other sellers on sites like Amazon,

⁸⁸ *Id.*

⁸⁹ https://www temu.com/about-temu.html?_x_vst_scene=adg&_x_ads_sub_channel=search&_x_ads_channel=google&_x_ads_account=1213016319&_x_ads_set=19694142866&_x_ads_id=141345685810&_x_ads_creative_id=648389974220&_x_ns_source=g&_x_ns_gclid=EAlaIQobChMIp-qu7uHrgQMVzOHjBx3NbwNPEAAAYASAAEgJG7vD_BwE&_x_ns_placement=&_x_ns_match_type=e&_x_ns_ad_position=&_x_ns_product_id=&_x_ns_target=&_x_ns_devicemodel=&_x_ns_wbraid=CjkKCQjwyY6pBhDkARIoAIxVarMMilmKANb_YPCex1QlQIP18Qo6VyWLb05bKiA0ncz9-bGx8hoCReg&_x_ns_gbraid=0AAAAAo4mICFRpdCyS3-Cw22MR1T_CF7V&_x_ns_keyword=temu&_x_ns_targetid=kwd-5681707004&refer_page_name=home&refer_page_id=10005_1696950675462_i3umf3qzlf&refer_page_sn=10005&_x_sessn_id=hbzdvdage0f.

⁹⁰ https://www.uscc.gov/sites/default/files/2023-04/Issue_Brief-Shein_Temu_and_Chinese_E-Commerce.pdf.

⁹¹ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

bearing no relationship to the actual goods being sold.⁹² In addition, while Defendants claim that they use “world-class manufacturers” and have a “zero tolerance policy against counterfeits,”⁹³ Temu frequently sells counterfeit, knock-off products in violation of the law. For example, it recently was reported that Temu was selling knockoff Air Jordans on the site and continued to do so even after the issue came to light.⁹⁴

109. In addition, while Defendants claim that they seek to “[d]o good for the world,” are “honest, ethical and trustworthy”, and are “socially responsible,”⁹⁵ a recent report found that much of the merchandise sold on Temu is produced using forced labor provided by China’s Uyghur minority held against their will in camps in the Chinese province of Xinjiang.⁹⁶ As the *Los Angeles Times* noted in a recent exposé, such practices are not only deceptive, but they violate federal law: “Products made in China’s western province of Xinjiang are being sold to U.S. consumers through

⁹² <https://www.businessinsider.com/temu-sellers-are-counterfeiting-amazon-listings-and-storefronts-2023-7>.

⁹³ https://www temu.com/confidence.html?_x_vst_scene=adg&_x_ads_sub_channel=search&_x_ads_channel=google&_x_ads_account=1213016319&_x_ads_set=19694142866&_x_ads_id=141345685810&_x_ads_creative_id=648389974220&_x_ns_source=g&_x_ns_gclid=EAIaIQobChMIpu7uHrgQMVzOHjBx3NbwnPEAAAYASAAEgJG7vD_BwE&_x_ns_placement=&_x_ns_match_type=e&_x_ns_ad_position=&_x_ns_product_id=&_x_ns_target=&_x_ns_devicemodel=&_x_ns_wbraid=CjkKCQjwyY6pBhDkARIoAIxVarMMilMKANb_YPCex1QIQIP18Qo6VyWLB05bKiA0ncz9-bGx8hoCReg&_x_ns_gbraid=0AAAAAo4mICFRpdcyS3-Cw22-MR1T_CF7V&_x_ns_keyword=temu&_x_ns_targetid=kwd-5681707004&refer_page_name=home&refer_page_id=10005_1696950675462_i3umf3qzlf&refer_page_sn=10005&_x_sessn_id=hbzdvdage0f.

⁹⁴ <https://www.businessinsider.com/shein-and-temu-listed-fake-air-jordans-for-under-50-2023-6>.

⁹⁵ https://www temu.com/about-temu.html?_x_vst_scene=adg&_x_ads_sub_channel=search&_x_ads_channel=google&_x_ads_account=1213016319&_x_ads_set=19694142866&_x_ads_id=141345685810&_x_ads_creative_id=648389974220&_x_ns_source=g&_x_ns_gclid=EAIaIQobChMIp-qu7uHrgQMVzOHjBx3NbwnPEAAAYASAAEgJG7vD_BwE&_x_ns_placement=&_x_ns_match_type=e&_x_ns_ad_position=&_x_ns_product_id=&_x_ns_target=&_x_ns_devicemodel=&_x_ns_wbraid=CjkKCQjwyY6pBhDkARIoAIxVarMMilMKANb_YPCex1QIQIP18Qo6VyWLB05bKiA0ncz9-bGx8hoCReg&_x_ns_gbraid=0AAAAAo4mICFRpdcyS3-Cw22-MR1T_CF7V&_x_ns_keyword=temu&_x_ns_targetid=kwd-5681707004&refer_page_name=home&refer_page_id=10005_1696950675462_i3umf3qzlf&refer_page_sn=10005&_x_sessn_id=hbzdvdage0f.

⁹⁶ <https://www.latimes.com/business/story/2023-06-15/temu-sells-products-linked-to-forced-labor-in-china>.

the online shopping platform Temu, in breach of a ban that forbids goods from the region due to links to forced labor, according to research by a global supply chain verification firm.” As one expert noted in the article, “It’s a systematic violation of U.S. trade policies.”⁹⁷

110. As the article explains, “Citing what the U.S. State Department has called ‘horrific abuses’ against the Uyghur people of Xinjiang, who are predominantly Muslim, federal officials banned the importation of cotton from the region in 2021 and expanded the law and its enforcement to all Xinjiang products last year under the Uyghur Forced Labor Prevention Act. Statements from former detainees and reports from an array of researchers and advocacy groups have alleged that the Chinese government put more than 1 million people in detention camps in the region and that laborers in fields and factories were forced or coerced.”⁹⁸

111. The U.S. government has also expressed concerns that Temu is selling Chinese goods to consumers in the United States that are manufactured using forced labor. For example, the Congressional U.S.-China Economic and Security Review Commission issued a report noting that Temu posed “risks and challenges to U.S. regulations, laws and principles of market access” resulting from such direct-to-consumer sales.⁹⁹ Likewise, Representative Mike Gallagher, chair of the House Select Committee on the Chinese Communist Party, and the panel’s top Democrat, Raja Krishnamoorthi, who represents Illinois’ 8th Congressional district, sent letters to Temu asking for information concerning whether the company is importing products derived from forced labor in China.

⁹⁷ *Id.*

⁹⁸ *Id.*

⁹⁹ <https://www.uscc.gov/research/shein-temu-and-chinese-e-commerce-data-risks-sourcing-violations-and-trade-loopholes>.

112. The House Select Committee on the Chinese Communist Party recently issued an Interim Report regarding its findings to date, entitled “Fast Fashion and the Uyghur Genocide.” The report concludes that “Temu does not have any system to ensure compliance with the Uyghur Forced Labor Prevention Act (UFLPA). This all but guarantees that shipments from Temu containing products made with forced labor are entering the United States on a regular basis, in violation of the UFLPA.”¹⁰⁰ The report concluded that Temu is actively seeking to avoid the protections in place to prevent the sale of goods manufactured with forced labor: “Temu’s business model ... is to avoid bearing responsibility for compliance with the UFLPA and other prohibitions on forced labor while relying on tens of thousands of Chinese suppliers to ship goods direct to U.S. consumers.”¹⁰¹ Moreover, the report observed that “Temu admitted that it does not expressly prohibit third party sellers from selling products based on their origin in the Xinjiang Autonomous Region.”¹⁰²

113. The committee’s report was issued after it held hearings at which it received expert testimony regarding the “genocide of the Uyghur people and other minorities.” As recounted in the report, “The Committee received first-hand witness testimony and expert reports about the CCP’s atrocities, which include imprisonment, torture, rape, forced sterilization, and the widespread exploitation of the Uyghur people in forced labor.”¹⁰³

114. The committee noted that the hearings provided evidence that Temu ships “millions of packages” to the United States “duty free” and “without providing CBP [Customs &

¹⁰⁰ <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fast-fashion-and-the-uyghur-genocide-interim-findings.pdf>.

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ *Id.*

Border Patrol] with sufficient data regarding the contents of the packages.”¹⁰⁴ The committee concluded: “In light of the sheer volume of shipments sent to the United States through its website, Temu’s failure to take any meaningful steps with respect to preventing the importation of goods with forced labor is striking.”¹⁰⁵

115. These unscrupulous practices have allowed Defendants to maximize their access to user data through the false promise of low-cost, high-quality goods. Moreover, they further demonstrate that Defendants’ real business is not providing a platform for the sale of quality merchandise, but rather obtaining access to user data under false pretenses, which they then misappropriate and seek to monetize.

116. Defendants utilize additional deceptive marketing techniques to induce users to sign up for the platform and grant Defendants access to user data. For example, Defendants run what has been described as an “affinity scam” or “chain letter” like tactic where users are repeatedly urged to sign up their friends and acquaintances in order to expand the number of users whose data Defendants may then access through the app.

117. Among other things, Temu offers credit and free items to users who get their friends and acquaintances to sign up for the app. “Those who do register are subjected to a bombardment of emails and app notifications.”¹⁰⁶ “[O]nce you give TEMU your personal information, you will be repeatedly spammed, hounded, nagged, and bribed to get your friends and family to give TEMU their personal information. When users fall down this rabbit hole

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ <https://web.archive.org/web/20230705172831/https://www.telegraph.co.uk/business/2023/07/01/temu-china-bargain-basement-amazon-rival-retail-online-shop/>.

(getting that Nintendo Switch absolutely free), TEMU sends a torrent of popup sequences milking users for ‘just one more contact’.”¹⁰⁷ In addition, Temu users are bombarded by notifications and spam from third parties other than Defendants. These emails and notifications occur even after users delete the app from their devices and even when users seek to block such notifications.

118. Moreover, Temu has utilized online “influencers” to harvest new users on an even larger scale. “There are now literally thousands of so-called ‘influencers’ hawking TEMU referrals on Reddit, YouTube, TikTok, and also Minecraft, Roblox, Discord... the pitch is: ‘You don’t have to buy anything, just sign up!’” “If you have a social media presence, TEMU will figure that out and will start to spam you – every day – to induce you to create videos promoting TEMU, for which they promise to pay.”¹⁰⁸

119. Defendants attract and maintain users through other fraudulent means. For example, “TEMU ... compensates users to write reviews,” which are then “obviously skewed positive.” Moreover, reviews are categorized in a deceptive manner with reviews characterized as “five star” positive reviews when in reality they contain extremely negative comments about the platform. For example, one report cited a so-called “five star” review stating that “What this company is doing is illegal” and constitutes “fraud”, that the company relies on “lies and deceptions”, and that “[c]ountless reviews are clearly negative, yet it shows that the person gave the item 5 stars which is impossible.”¹⁰⁹

¹⁰⁷ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

¹⁰⁸ *Id.*

¹⁰⁹ *Id.*

120. Finally, as illustrated by its gamified nature, Temu is designed to be highly addictive. As one report notes, “[t]he app successfully keeps people hooked. The average user spends around 28 minutes a day on the app, according to Sensor Tower, nearly double the 16 minutes spent on Amazon.”¹¹⁰ The more time users spend on the app, the more data is available for covert collection by Defendants in violation of users’ right to privacy in their personal data.

121. As one analysis observes, the addictive tactics extend not only to users’ continued use of the platform, but also inducing individuals to sign up for the app: “Your behavior will be categorized and siloed. If these kinds of inducements exert an addictive pull on your brain, AI pattern recognition will guarantee you will see a lot more of them. If you are on the TEMU website, all the most persistent inducements are pointed towards getting you to install the TEMU app.”¹¹¹

F. Additional Allegations Concerning the Named Plaintiffs

122. During the time that the Temu app was installed on the named plaintiffs’ mobile devices, Defendants surreptitiously performed, among others, the following actions without notice to or the knowledge and consent of the named plaintiffs or, in the case of the minor plaintiffs, their legal guardians: (i) Defendants took plaintiffs’ user/device identifiers and private data from their mobile devices; (ii) Defendants took plaintiffs’ biometric identifiers and information from plaintiffs’ mobile devices; (iii) Defendants took plaintiffs’ private and personally identifiable data and content from plaintiffs’ mobile devices; and (iv) Defendants made some or all such stolen data

¹¹⁰ <https://web.archive.org/web/20230705172831/https://www.telegraph.co.uk/business/2023/07/01/temu-china-bargain-basement-amazon-rival-retail-online-shop/>.

¹¹¹ <https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/>.

and content accessible to individuals in China – including individuals under the control of the Chinese government.

123. Defendants performed these acts for the purpose of secretly collecting the named plaintiffs’ private and personally identifiable data and content – including their user/device identifiers, biometric identifiers and information, and other private information – and using such data and content to track, profile and target plaintiffs with advertisements. Further, Defendants have used plaintiffs’ private and personally identifiable data and content for their economic gain. Defendants and others now have access to private and personally identifiable data and content regarding plaintiffs that can be used for further commercial advantage and other harmful purposes. Defendants have profited, and will continue to profit, from these activities.

124. Meanwhile, the named plaintiffs have incurred harm as a result of Defendants’ invasion of their privacy rights through Defendants’ covert taking of plaintiffs’ private and personally identifiable data and content – including their user/device identifiers, biometric identifiers and information, and private information and data. Plaintiffs also have suffered harm because Defendants’ actions have diminished the value of their private and personally identifiable data and content. Moreover, plaintiffs have suffered injury to their mobile devices. The battery, memory, CPU, and bandwidth of such devices have been compromised, and as a result, the functioning of those devices has been impaired and slowed, due to Defendants’ clandestine and unlawful activities. Finally, Plaintiffs have incurred additional data usage and electricity costs that they and/or their guardians would not have incurred but for Defendants’ covert and unlawful actions.

125. Neither the named plaintiffs nor, in the case of the minor plaintiffs, their guardians, ever received notice that Defendants would collect, capture, receive, otherwise obtain, store, and/or use their biometric identifiers and other private information. Defendants never informed plaintiffs or their guardians of the specific purpose and length of time for which their biometric identifiers or other biometric information would be collected, captured, received, otherwise obtained, stored, and/or used. Neither Plaintiffs nor, in the case of minors, their guardians, ever signed a written release authorizing Defendants to collect, capture, receive, otherwise obtain, store, and/or use their biometric identifiers or other biometric information.

126. Based on counsel's investigation and analysis, Temu deliberately designed its Terms of Service and Privacy Policy to decrease the likelihood that a user will notice and comprehend its terms and conditions or could provide meaningful, express consent to its conditions, in order to encourage users to sign up and not be deterred by accurate and truthful disclosures.

127. The named plaintiffs did not know nor expect that Defendants would collect, store, and use their biometric identifiers and biometric information when they used the Temu app.

128. The named plaintiffs did not receive notice from Defendants (written or otherwise) that Defendants would collect, store, and/or use their biometric identifiers or biometric information. Plaintiffs did not receive notice from Defendants of the specific purpose and length of time that Defendants would collect, store, and/or use their biometric identifiers or biometric information. Plaintiffs did not give authorization (written or otherwise) for Defendants to collect, store, and/or use their biometric identifiers or biometric information.

V. CLASS ALLEGATIONS

129. Plaintiffs seek certification of the classes set forth herein pursuant to Federal Rule of Civil Procedure 23 (“Rule 23”). Specifically, Plaintiffs seek class certification of all claims for relief herein on behalf of a class and subclasses defined as follows:

Nationwide Class: All persons who reside in the United States who used the Temu platform.

Illinois Subclass: All persons who reside in Illinois and used the Temu platform.

California Subclass: All persons who reside in California and used the Temu platform.

Virginia Subclass: All persons who reside in Virginia and used the Temu platform.

130. Plaintiffs are the proposed class representatives for the Nationwide Class. California Plaintiffs are the proposed class representatives for the California Subclass. Illinois Plaintiffs are the proposed class representatives for the Illinois Subclass. Virginia Plaintiffs are the proposed representatives for the Virginia Subclass.

131. Plaintiffs reserve the right to modify or refine the definitions of the Class and the Subclasses.

132. Excluded from the Class and the Subclasses are: (i) any judge or magistrate judge presiding over this action and members of their staff, as well as members of their families; (ii) Defendants, Defendants’ predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which any Defendant or its parents have a controlling interest, as well as Defendants’ current or former employees, agents, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the class; (iv) persons whose claims in this matter have been

finally adjudicated on the merits or otherwise released; (v) counsel for Defendants; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

133. **Ascertainability.** The proposed Class and Subclasses are readily ascertainable because they are defined using objective criteria so as to allow Class and Subclass members to determine if they are part of the Class and/or one of the Subclasses. Further, the Class and Subclasses can be readily identified through records maintained by Defendants.

134. **Numerosity (Rule 23(a)(1)).** The Class and Subclasses are so numerous that joinder of individual members herein is impracticable. The exact number of Class and Subclass members, as herein identified and described, is not known, but download figures indicate that the Temu app has been downloaded at least 100 million times.

135. **Commonality (Rule 23(a)(2)).** Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class and Subclass members, including the following:

- a) Whether Defendants engaged in the activities and practices referenced above;
- b) Whether Defendants' activities and practices referenced above constitute a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
- c) Whether Defendants' activities and practices referenced above constitute a violation of the Federal wiretap statute, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 *et seq.*;
- d) Whether Defendants' activities and practices referenced above constitute a violation of the right of privacy under Mass. Gen. Laws Ch. 214, § 1B;

- e) Whether Defendants' activities and practices referenced above constitute a violation of the Massachusetts Wiretap Act, Mass. Gen. Laws, Ch. 272, § 99;
- f) Whether Defendants' activities and practices referenced above constitute unjust enrichment concerning which restitution and/or disgorgement is warranted;
- g) Whether Defendants' activities and practices referenced above constitute a violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*;
- h) Whether Defendants' activities and practices referenced above constitute a violation of the California Comprehensive Data Access and Fraud Act, Cal. Pen. C. § 502;
- i) Whether Defendants' activities and practices referenced above constitute a violation of the right of privacy under the California Constitution;
- j) Whether Defendants' activities and practices referenced above constitute intrusion upon seclusion;
- k) Whether Defendants' activities and practices referenced above constitute a violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200 *et seq.*;
- l) Whether Defendants' activities and practices referenced above constitute a violation of the California False Advertising Law, Bus. & Prof. C. §§ 17500 *et seq.*;
- m) Whether Defendants' activities and practices referenced above constitute a violation of the Virginia Computer Crimes Act, Va. Code § 18.2-152.1, *et seq.*
- n) Whether Plaintiffs and members of the Class and Subclasses sustained damages as a result of Defendants' activities and practices referenced above, and, if so, in what amount;

- o) Whether Defendants profited from their activities and practices referenced above, and, if so, in what amount;
- p) What is the appropriate injunctive relief to ensure that Defendants no longer unlawfully: (i) take private and personally identifiable Temu user data and content – including user/device identifiers, biometric identifiers and information, and other private and personally identifiable data; (ii) utilize private and personally identifiable Temu user data; (iii) utilize private and personally identifiable Temu user data and content to create consumer demand for and use of Defendants’ other products; (iv) give access to such private and personally identifiable Temu user data and content to individuals in China and to third parties either in China or whose data is accessible from within China; (v) cause the diminution in value of Temu users’ private and personally identifiable data; (vi) cause injury and harm to Temu users’ mobile devices; (vii) cause Temu users to incur higher data usage and electricity charges; (viii) retain the unlawfully acquired private and personally identifiable data of Temu users; and (ix) profile and target, based on the above activities, Temu users with advertisements; and
- q) What is the appropriate injunctive relief to ensure that Defendants take reasonable measures to ensure that they and relevant third parties destroy unlawfully acquired private and personally identifiable Temu user data in their possession, custody or control.

136. **Typicality (Rule 23(a)(3)).** Plaintiffs’ claims are typical of the claims of members of the Class and Subclasses because, among other things, Plaintiffs and members of the Class and

Subclasses sustained similar injuries as a result of Defendants' uniform wrongful conduct, and their legal claims all arise from the same events and wrongful conduct by Defendants.

137. **Adequacy (Rule 23(a)(4)).** Plaintiffs will fairly and adequately protect the interests of the Class and Subclasses. Plaintiffs' interests do not conflict with the interests of the Class and Subclass members, and Plaintiffs have retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the Class and Subclasses.

138. **Predominance & Superiority (Rule 23(b)(3)).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class and Subclass members, and a class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. The amount of damages available to Plaintiffs is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense presented by the complex legal and factual issues of the case to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

139. **Final Declaratory or Injunctive Relief (Rule 23(b)(2)).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). Defendants have acted or refused to act on grounds that apply generally to the Class and Subclasses, making final declaratory and/or injunctive relief appropriate with respect to the Class and Subclasses as a whole.

VI. APPLICABLE LAW

140. In addition to any state-specific claims they may have (such as the Illinois BIPA claims brought by the Illinois Subclass), every member of the class may invoke Massachusetts' substantive laws to bring claims against Defendants, regardless of where in the United States the Class Member resides. Massachusetts' substantive laws may be constitutionally applied to the claims of Plaintiffs and the Class under the Due Process Clause, 14th Amend. §1, and the Full Faith and Credit Clause, Art. IV §1 of the U.S. Constitution. Massachusetts has significant contacts, or significant aggregation of contacts, to the claims asserted by Plaintiff and all Class Members, thereby creating state interests that ensure that the application of Massachusetts state law is not arbitrary or unfair.

141. Defendants' U.S. headquarters and principal place of business is located in Massachusetts. Defendants also own property and conduct substantial business in Massachusetts, and therefore Massachusetts has an interest in regulating Defendants' conduct under its laws. Defendants' decision to reside in Massachusetts and avail itself of Massachusetts' laws, and to engage in the challenged conduct from and emanating out of Massachusetts, renders the application of Massachusetts law to the claims herein constitutionally permissible.

142. Massachusetts is also the state from which Defendants' alleged misconduct emanated. This conduct similarly injured and affected Plaintiff and all other Class Members.

143. The application of Massachusetts laws to the claims of the Class is also appropriate under Massachusetts' choice of law rules because Massachusetts has significant contacts to the claims of Plaintiff and the proposed Class, and Massachusetts has a greater interest in applying its laws here than any other interested state.

VII. COUNTS

FIRST COUNT:

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030 (On Behalf of the Plaintiffs and the Class)

144. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

145. The Plaintiffs' and the Class's computers and mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

146. Defendants have exceeded, and continue to exceed, authorized access to the Plaintiffs' and the Class's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

147. Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), inter alia, because of the secret transmission of the Plaintiffs' and the Class's private and personally identifiable data and information – including user/device identifiers, biometric identifiers and information, and other private and personally identifiable data and information.

148. Defendants' conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of the Plaintiffs and the Class being made available to foreign actors, including foreign intelligence services, in locations without adequate legal privacy protections. That this threat is real and imminent is evidenced by the materials cited above.

149. Accordingly, the Plaintiffs and the Class are entitled to “maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.” 18 U.S.C. § 1030(g).

SECOND COUNT:

**VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986 (ECPA),
18 U.S.C. §§ 2510 *ET SEQ.*
(On Behalf of the Plaintiffs and the Class)**

150. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

151. The Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq.*, prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authority party to the communication. The statute confers a civil cause of action on “any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter.” 18 U.S.C. § 2520(a).

152. “Intercept” is defined as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4).

153. “Contents” is defined as “includ[ing] any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

154. “Person” is defined as “any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.” 18 U.S.C. § 2510(6).

155. “Electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,

electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce” 18 U.S.C. § 2510(12).

156. Defendants are each a “person” for purposes of the Wiretap Act because they are corporations.

157. As described above, the code used by the Temu app secretly accesses texts, emails and other content on users’ computers and thus constitutes a “device or apparatus” that is used to intercept a wire, oral, or electronic communication through electronic means.

158. Plaintiffs’ and Class Members’ sensitive personal information, data, and interactions with other individuals and websites that Defendants surreptitiously intercepted through the Temu app are “electronic communication[s]” under 18 U.S.C. § 2510(12).

159. Plaintiffs and Class Members reasonably believed that Defendants were not intercepting, recording, or disclosing their electronic communications.

160. Plaintiffs’ and Class Members’ electronic communications were intercepted during transmission, without their consent and for the unlawful and/or wrongful purpose of monetizing private information and data, including by using their private information and data to develop marketing and advertising strategies and utilizing user data for other commercial advantage.

161. Defendants were not parties to those communications, which occurred between Plaintiffs and Class Members and third parties or other websites they sought to access or accessed. Defendants used Plaintiffs’ and Class Members’ electronic communications as part of their business model.

162. Defendants’ actions were at all relevant times knowing, willful, and intentional, particularly because Defendants are sophisticated parties who know the type of data they intercept

through their own products. Moreover, experts who have examined the Temu app have concluded that the features of the app that allow these covert interceptions are intentional, non-trivial, engineering tasks—the kind that does not happen by mistake or randomly.

163. Neither Plaintiffs nor Class Members consented to Defendants' interception, disclosure, and/or use of their electronic communications. The third parties and/or websites that Plaintiffs and Class Members visited did not know of or consent to Defendants' interception of the communications. Nor could they—Defendants never sought to obtain, nor did they obtain, Plaintiffs', Class Members', or third parties' consent to intercept Temu users' electronic communications with third parties.

164. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are each entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made by Defendants as a result of the violation, or (b) statutory damages of whichever is the greater of \$100 per day per violation or \$10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

THIRD COUNT:

VIOLATION OF THE RIGHT TO PRIVACY UNDER MASS. GEN. LAWS CH. 214, § 1B (On Behalf of the Plaintiffs and the Class)

165. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

166. Mass. Gen. Laws Ch. 214, § 1B provides that “A person shall have a right against unreasonable, substantial or serious interference with his privacy.” The statute provides a private cause of action for damages by those whose privacy rights were violated.

167. Plaintiffs and the Class hold, and at all relevant times held, a legally protected privacy interest in their private and personally identifiable data and content – including user/device Identifiers, biometric identifiers and information, and other private information – on their mobile devices and computers.

168. There is a reasonable expectation of privacy concerning Plaintiffs’ and the Class’s data and content under the circumstances present.

169. As the materials cited above demonstrate, Defendants have engaged in unreasonable, substantial, and serious interference with Plaintiffs and Class Members’ privacy rights.

170. The reasonableness of Plaintiffs’ and the Class’s expectation of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendants’ taking of private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information – from Plaintiffs’ and the Class’s mobile devices and other social media accounts.

171. Defendants intentionally intruded upon the Plaintiffs’ and the Class’s solitude, seclusion, and private affairs – and continue to do so – by intentionally designing the Temu app, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain the Plaintiffs’ and the Class’s private and personally identifiable data and content –

including user/device identifiers, biometric identifiers and information, and other private data and information never intended for public consumption.

172. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

173. Defendants' conduct constitutes and, at all relevant times, constituted a serious invasion of privacy, as Defendants either did not disclose at all, or failed to make an effective disclosure, that they would take and make use of – and allow individuals and companies based in China to take and make use of – Plaintiffs' and the Class's private and personally identifiable data. Defendants intentionally invaded Plaintiffs' and the Class's privacy interests by intentionally designing the Temu app, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain their private and personally identifiable data and content. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

174. Defendants further violated Plaintiffs' and the Class's privacy rights by making Plaintiffs' and the Class's private and personally identifiable data and content available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The intentionality of Defendants' conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendants' conduct targeted Plaintiffs' and the Class's mobile devices, which the United States

Supreme Court has characterized as almost a feature of human anatomy, and which contain Plaintiffs' and the Class's private and personally identifiable data and information.

175. Plaintiffs and the Class were harmed by, and continue to suffer harm as a result of, the intrusion as detailed throughout this Complaint.

176. Defendants' conduct was a substantial factor in causing the harm suffered by Plaintiffs and the Class.

177. Plaintiffs and the Class seek compensatory and punitive damages as a result of Defendants' actions. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were calculated to injure the Plaintiffs and the Class and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

178. Plaintiffs and the Class seek injunctive relief to rectify Defendants' actions, including but not limited to requiring Defendants to stop taking more private and personally identifiable data and information of Plaintiffs and the Class from their mobile devices and computers than is reasonably necessary to operate the Temu app; to make clear disclosures; to obtain Plaintiffs' and the Class's consent to the taking of their private and personally identifiable data and information; to stop allowing individuals in China access to Plaintiffs' private and personally identifiable data and information; to stop transferring such information to servers that are accessible from within China; and to recall and destroy Plaintiffs' and the Class's private and personally identifiable data and information already taken in contravention of Plaintiffs' and the Class's right to privacy.

179. Plaintiffs and the Class seek restitution and disgorgement for Defendants' violation of their privacy rights. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

180. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (2nd) of Torts § 652B. 361. The Plaintiffs and the Class have, and at all relevant times had, a reasonable expectation of privacy in their mobile devices and computers. And their private affairs include their past, present and future activity on their mobile devices and computers.

FOURTH COUNT:

VIOLATION OF THE MASSACHUSETTS WIRETAP ACT, MASS. GEN. LAWS, CH. 272, § 99 (On Behalf of the Plaintiffs and the Class)

181. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

182. Mass. Gen. Laws, Ch. 272, § 99 provides that "Any aggrieved person whose oral or wire communications were intercepted, disclosed or used except as permitted or authorized by this section or whose personal or property interests or privacy were violated by means of an

interception except as permitted or authorized by this section shall have a civil cause of action against any person who so intercepts, discloses or uses such communications or who so violates his personal, property or privacy interest” *Id.* § 99.Q.

183. The term "wire communication" means “any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception.” *Id.* 99.B.1.

184. The term "interception" means “to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication....” *Id.* 99.B.4.

185. Defendants are each a “person” for purposes of the Wiretap Act because they are corporations.

186. As described above, the code used by the Temu app secretly accesses, texts, emails and other content on users’ computers and thus constitutes an “intercepting device” that is used to intercept a wire, oral, or electronic communication through electronic means.

187. Plaintiffs’ and Class Members’ sensitive personal information, data, and interactions with other individuals and websites, including texts, emails, and other communications, that Defendants secretly intercepted through the Temu app are “wire communications”.

188. Plaintiffs and Class Members reasonably believed that Defendants were not intercepting, recording, or disclosing their electronic communications. Defendants’ interception of Plaintiffs’ and the Class’s communications was done in secret.

189. Plaintiffs' and Class Members' electronic communications were intercepted during transmission, without their consent and for the unlawful and/or wrongful purpose of monetizing private information and data, including by using their private information and data to develop marketing and advertising strategies and utilizing user data for other commercial advantage.

190. Defendants were not parties to those communications, which occurred between Plaintiffs and Class Members and third parties or other websites they sought to access or accessed. Defendants used Plaintiffs' and Class Members' electronic communications as part of their business model.

191. Defendants' actions were at all relevant times knowing, willful, and intentional, particularly because Defendants are sophisticated parties who know the type of data they intercept through their own products. Moreover, experts who have examined the Temu app have concluded that the features of the app that allow these covert interceptions are intentional, non-trivial, engineering tasks—the kind that does not happen by mistake or randomly. These experts also concluded that Defendants sought to conceal the features of the Temu app that accomplished the interception of Plaintiffs' and the Class's communications.

192. Neither Plaintiffs nor Class Members consented to Defendants' interception, disclosure, and/or use of their electronic communications. The third parties and/or websites that Plaintiffs and Class Members visited did not know of or consent to Defendants' interception of the communications. Nor could they—Defendants never sought to obtain, nor did it obtain, Plaintiffs', Class Members', or third parties' consent to intercept Temu users' electronic communications with third parties.

193. Pursuant to Mass. Gen. Laws, Ch. 272, § 99Q, Plaintiffs and Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are each entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made by Defendants as a result of the violation, or (b) statutory damages of whichever is the greater of \$100 per day per violation or \$1,000; (3) punitive damages; and (4) reasonable attorneys' fees and other litigation disbursements reasonably incurred.

FIFTH COUNT:

**RESTITUTION / UNJUST ENRICHMENT
(On Behalf of the Plaintiffs and the Class)**

194. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

195. Plaintiffs and the Class have conferred substantial benefits on Defendants by downloading and using the Temu app. These include the Defendants' collection and use of the Plaintiffs' and the Class's private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information never intended for public consumption. Such benefits also include the revenues and profits resulting from Defendants' collection and use of such data and content for Defendants' targeted-advertising, use of the data, and increased consumer demand for and use of Defendants' products.

196. Defendants possess user/device identifiers, biometric identifiers and information, and other highly personal data sufficient to create a dossier of private and personally identifiable

data and content for each Temu user. Such living files can be supplemented over time with additional private and personally identifiable user data and content, and all of this private and personally identifiable data and information has been, is, and will be used in the past, the present, and the future for Defendants' economic and financial gain.

197. Defendants' unlawful possession and control over this data and information make tracking and profiling Temu users, and targeting them with advertising, much more efficient, effective, and lucrative. Such private and personally identifiable data and content are used to analyze Temu users' income, consumption habits, and preferences. Such information provides guidance as to what methods of advertising will be most effective on particular Temu users, what products – including Defendants' own products – will be most attractive to particular Temu users, and how much to spend on particular ads. Defendants unjustly have earned and continue to earn substantial profits and revenues from such targeted advertising and from generating increased demand for and use of Defendants' other products.

198. Analysts have observed that, based on the features and design of the Temu app, Defendants may be utilizing the app to purposefully harvest user data for subsequent resale to third parties without Plaintiffs' consent, thereby deriving further economic advantage.

199. Meanwhile, Plaintiffs, the Class and the Subclasses have incurred, and continue to incur, harm as a result of the invasion of privacy stemming from Defendants' covert theft of their private and personally identifiable data and content – including their user/device identifiers, biometric identifiers and information, and other highly personal information. These injuries are further exacerbated by the fact that Plaintiffs' user data is available to the Chinese communist government which, by law, now has access to Plaintiffs' data without Plaintiffs' consent.

200. Plaintiffs, the Class and the Subclasses also have suffered and continue to suffer harm in the form of diminution of the value of their private and personally identifiable data and content as a result of Defendants' surreptitious and unlawful activities.

201. Moreover, Plaintiffs, the Class and the Subclasses have suffered and continue to suffer injuries to their mobile devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed, due to Defendants' clandestine and unlawful activities.

202. Plaintiffs, the Class, and the Subclasses have incurred additional data usage and electricity costs that they would not have incurred but for Defendants' covert and unlawful actions.

203. Defendants have knowingly and willingly accepted and enjoyed these benefits.

204. Defendants either knew or should have known that the benefits rendered by the Plaintiffs and the Class were given with the expectation that Defendants would not take and use the Plaintiffs' and the Class's private and personally identifiable data and content that Defendants have taken and used without permission. For Defendants to retain the aforementioned benefits under these circumstances is inequitable.

205. Through deliberate violation of the Plaintiffs' and the Class's privacy interests, and statutory and constitutional rights, Defendants each reaped benefits that resulted in each Defendant wrongfully receiving profits. Likewise, Defendants received significant benefits as a result of their intentionally deceptive and unfair business practices.

206. Equity demands disgorgement of Defendants' ill-gotten gains. Defendants will be unjustly enriched unless they are ordered to disgorge those profits for the benefit of the Plaintiffs and the Class.

207. As a direct and proximate result of Defendants' wrongful conduct and unjust enrichment, the Plaintiffs and the Class are entitled to restitution from Defendants and institution of a constructive trust disgorging all profits, benefits, and other compensation obtained by Defendants through this inequitable conduct.

SIXTH COUNT:

**VIOLATION OF ILLINOIS'S BIOMETRIC INFORMATION PRIVACY ACT, 740 ILCS 14/1, *ET SEQ.*
(On Behalf of the Illinois Plaintiffs and the Illinois Subclass)**

208. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

209. Defendants are violating specific statutory protections governing biometric data contained in the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.* In 2008, Illinois enacted BIPA to address the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Ses. No. 276. The Illinois Legislature recognized the importance of protecting the privacy of individuals' biometric data, finding that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse [and] is at heightened risk for identity theft" *Id.* 239. As the Illinois Supreme Court has recognized, through BIPA, "our General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197, 1206 (Ill. 2019).

210. BIPA thus focuses on “biometric identifiers” and “biometric information.”

Biometric identifiers consist of “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10. A “scan” under BIPA means to examine by observation or checking, or systematically in order to obtain data especially for display or storage. *In re Facebook Biometric Information Privacy Litigation*, 2018 WL 2197546, *3 (N.D. Cal. May 14, 2018).

“Geometry” under BIPA is the relative arrangement of parts or elements. *Id.* Neither the term “scan” nor the term “geometry” requires “actual or express measurements of spatial quantities like distance, depth, or angles.” *Id.* Biometric information constitutes “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.” 740 ILCS 14/10.

211. BIPA makes it unlawful for any private entity to, among other things, “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject’s legally authorized representative.” 740 ILCS 14/15(b). At all relevant times, the Illinois Plaintiffs were residents of Illinois and each is a “person” and/or a “customer” within the meaning of BIPA. 740 ILCS 14/15(b)..

212. Each Defendant is, and at all relevant times was, a “corporation, limited liability company, association, or other group, however organized,” and thus is, and at all relevant times was, a “private entity” under the BIPA. 740 ILCS 14/10.

213. The Illinois Plaintiffs and the Illinois Subclass had their “biometric identifiers,” including their “biometric information” collected, captured, received, or otherwise obtained by Defendants as a result of the Illinois Plaintiffs’ and the Illinois Subclass’s use of the Temu app. 740 ILCS 14/10.

214. At all relevant times, Defendants systematically and surreptitiously collected, captured, received or otherwise obtained the Illinois Plaintiffs’ and the Illinois Subclass’s “biometric identifiers” and “biometric information” without first obtaining signed written releases, as required by 740 ILCS 14/15(b)(3), from any of them or their “legally authorized representatives.”

215. In fact, Defendants failed to properly inform the Illinois Plaintiffs and the Illinois Subclass, or any of their parents, legal guardians, or other “legally authorized representatives,” in writing (or in any other way) that the Illinois Plaintiffs’ and the Illinois Subclass’s “biometric identifiers” and “biometric information” were being “collected or stored” by Defendants. Nor did Defendants inform the Illinois Plaintiffs and the Illinois Subclass, or any of their parents, legal guardians, or other “legally authorized representatives,” in writing of the specific purpose and length of term for which the Illinois Plaintiffs’ and the Illinois Subclass’s “biometric identifiers” and “biometric information” were being “collected, stored and used” as required by 740 ILCS 14/15(b)(1)-(2).

216. Defendants' unauthorized collection of users' biometric data is particularly harmful here given the access that the Chinese government has to such data. The Chinese government has aggressively sought to collect such data and information in order to further the country's advances in artificial intelligence.

217. As the South China Morning Post reported: "China's goal of becoming a global leader in artificial intelligence (AI) is nowhere more manifested than in how facial recognition technology has become a part of daily life in the world's second-largest economy. Facial recognition systems, which are biometric computer applications that automatically identify an individual from a database of digital images, are now being used extensively in areas such as public security, financial services, transport and retail across the country."¹¹² In fact, the Chinese government employs a variety of biometrics for population surveillance and control: "In addition to voice recognition, there are facial and pupil recognition, gathering of DNA samples—building the world's largest DNA database—and fingerprint scans."¹¹³

218. BIPA also makes it unlawful for a private entity "in possession of a biometric identifier or biometric information" to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

219. Defendants are, and at all relevant times were, "in possession of" the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers," including but not limited to their "biometric information." Defendants profited from such "biometric identifiers" and "biometric

¹¹² <https://www.scmp.com/tech/start-ups/article/2133234/meet-five-chinese-start-ups-pushing-facial-recognition-technology>.

¹¹³ <https://vlifestyle.org/codec-news/?l=business/content-2254742-china-gathers-peoples-voices-new-identification-technology-drawing-concerns>.

information” by using them for targeted advertising and the generation of increased demand for and use of Defendants’ other products. 740 ILCS 14/15(c).

220. Finally, BIPA prohibits private entities “in possession of a biometric identifier or biometric information” from “disclos[ing], redisclos[ing], or otherwise disseminat[ing] a person’s or a customer’s biometric identifier or biometric information unless” any one of four enumerated conditions are met. 740 ILCS 14/15(d)(1)-(4). None of such conditions are met here.

221. Defendants disclose, redisclose and disseminate, and at all relevant times disclosed, redisclosed and disseminated, the Illinois Plaintiffs’ and the Illinois Subclass’s “biometric identifiers,” including but not limited to their “biometric information” without the consent of any of them or their “legally authorized representatives.” 740 ILCS 14/15(d)(1). Moreover, the disclosures and redisclosures did not “complete[] a financial transaction requested or authorized by” the Illinois Plaintiffs, the Illinois Subclass or any of their legally authorized representatives. 740 ILCS 14/15(d)(2). Nor are, or at any relevant times were, the disclosures and redisclosures “required by State or federal law or municipal ordinance.” 740 ILCS 14/15(d)(3). Finally, at no point in time were the disclosures ever “required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.” 740 ILCS 14/15(d)(4). BIPA mandates that a private entity “in possession of biometric identifiers or biometric information” “develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual’s last interaction with the private entity, whichever occurs first.” 740 ILCS 14/15(a). But Defendants do not publicly provide any written policy establishing any retention schedule or

guidelines for permanently destroying the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information." 740 ILCS 14/15(a).

222. BIPA also commands private entities "in possession of a biometric identifier or biometric information" to: (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits and protects other confidential and sensitive information. 740 ILCS 14/15(e). Based on the facts alleged herein, including Defendants' lack of an adequate public written policy, their failure to inform Temu users that Defendants obtain such users' "biometric identifiers" and "biometric information," their failure to obtain written consent to collect or otherwise obtain Temu users' "biometric identifiers" and "biometric information," and their unauthorized dissemination of Temu users' "biometric identifiers" and "biometric information," Defendants have violated this provision too.

223. Defendants recklessly or intentionally violated each of BIPA's requirements and infringed the Illinois Plaintiffs' and the Illinois Subclass's rights to keep their immutable and uniquely identifying biometric identifiers and biometric information private. As individuals subjected to each of Defendants' BIPA violations above, the Illinois Plaintiffs and the Illinois Subclass are and have been aggrieved. 740 ILCS 14/20.

224. On behalf of themselves and the Illinois Subclass, the Illinois Plaintiffs seek: (1) injunctive and equitable relief as is necessary to protect the interests of the Illinois Plaintiffs and the Illinois Subclass by requiring Defendants to comply with BIPA's requirements; (2) \$1,000.00

or actual damages, whichever is greater, for each negligent violation of BIPA by Defendants; (3) \$5,000.00 or actual damages, whichever is greater, for each intentional or reckless violation of BIPA by Defendants; and (4) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses. 740 ILCS 14/20(1)-(4).

SEVENTH COUNT:

**VIOLATION OF THE CALIFORNIA COMPREHENSIVE DATA ACCESS AND FRAUD ACT,
CAL. PEN. C. § 502
(On Behalf Of the California Plaintiffs and California Subclass)**

225. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

226. Defendants' acts violate Cal. Pen. C. § 502(c)(1) because they have knowingly accessed, and continue to knowingly access, data and computers to wrongfully control or obtain data. The Plaintiffs' and the Subclass's private and personally identifiable data and content accessed by Defendants – including user/device identifiers, biometric identifiers and information, and other private data – far exceeds any reasonable use of the Plaintiffs' and the Subclass's data and content to operate the Temu app. There is no justification for Defendants' surreptitious collection and transfer of the Plaintiffs' and the Subclass's private and personally identifiable data and content from their devices and computers and allowing access to that information to individuals and third-party companies in China that are subject to Chinese law requiring the sharing of such data and content with the Chinese government.

227. Defendants' acts violate Cal. Pen. C. § 502(c)(2) because they have knowingly accessed and without permission taken, copied, and made use of data from a computer – and they continue to do so. Defendants did not obtain permission to take, copy, and make use of the

Plaintiffs’ and the Subclass’s private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information – from their devices – and provide access to individuals and companies that are subject to Chinese law requiring the sharing of such data and content with the Chinese government.

228. Accordingly, the Plaintiffs and the Subclass are entitled to compensatory damages, including “any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access,” injunctive relief, and attorneys’ fees. Cal. Pen. C. § 502(e)(1), (2).

EIGHTH COUNT:

VIOLATION OF THE RIGHT OF PRIVACY UNDER THE CALIFORNIA CONSTITUTION (On Behalf Of the California Plaintiffs and California Subclass)

229. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

230. Plaintiffs and the California Subclass hold, and at all relevant times held, a legally protected privacy interest in their private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data – on their devices and computers.

231. There is a reasonable expectation of privacy concerning Plaintiffs’ and the Subclass’s data and content under the circumstances present.

232. The reasonableness of Plaintiffs’ and the Subclass’s expectation of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendants’ accessing private

and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information – from Plaintiffs’ and the Subclass’s devices and computers.

233. Defendants’ conduct constitutes and, at all relevant times, constituted a serious invasion of privacy, as Defendants either did not disclose at all, or failed to make an effective disclosure, that they would take and make use of – and allow individuals and companies based in China to take and make use of – Plaintiffs’ and the Subclass’s private and personally identifiable data and content. Defendants intentionally invaded Plaintiffs’ and the Subclass’s privacy interests by intentionally designing the Temu app, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain their private and personally identifiable data and content. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendants’ intrusion is heightened by Defendants’ making Plaintiffs’ and the Subclass’s private and personally identifiable data and content available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The intentionality of Defendants’ conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendants’ conduct targeted Plaintiffs’ and the Subclass’s devices, which contain Plaintiffs’ and the Subclass’s private and personally identifiable data and content.

234. Plaintiffs and the Subclass were harmed by, and continue to suffer harm as a result of, the intrusion as detailed throughout this Complaint.

235. Defendants' conduct was a substantial factor in causing the harm suffered by Plaintiffs and the Subclass.

236. Plaintiffs and the Subclass seek compensatory and punitive damages as a result of Defendants' actions. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were calculated to injure the Plaintiffs and the Subclass and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

237. Plaintiffs and the Subclass seek injunctive relief to rectify Defendants' actions, including but not limited to requiring Defendants (a) to stop taking more private and personally identifiable data and content of Plaintiffs and the Subclass from their devices and computers than is reasonably necessary to operate the Temu app; (b) to make clear disclosures of Plaintiffs' and the Subclass's private and personally identifiable data and content that is reasonably necessary to operate the Temu app; (c) to obtain Plaintiffs' and the Subclass's consent to the taking of their private and personally identifiable data and content; (d) to stop providing access to the Plaintiffs' private and personally identifiable data and content to individuals in China or transferring such data to servers or companies whose data is accessible from within China; and (e) to recall and destroy Plaintiffs' and the Subclass's private and personally identifiable data and content already taken in contravention of Plaintiffs' and the Subclass's right to privacy under the California Constitution.

238. The Plaintiffs and the Subclass seek restitution and disgorgement for Defendants' violation of their privacy rights. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters

the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes “conscious interference with a claimant’s legally protected interests,” including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

NINTH COUNT:

**INTRUSION UPON SECLUSION
(On Behalf Of the California Plaintiffs and California Subclass)**

239. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

240. “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” Restatement (2nd) of Torts § 652B.

241. The Plaintiffs and the California Subclass have, and at all relevant times had, a reasonable expectation of privacy in their devices and computers, and their private affairs include their past, present and future activity on their devices and their other media accounts.

242. The reasonableness of the Plaintiffs’ and the Subclass’s expectations of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendants’ taking of private and personally identifiable data and content from the Plaintiffs’ and the Subclass’s devices and computers.

243. Defendants intentionally intruded upon the Plaintiffs’ and the Subclass’s solitude, seclusion, and private affairs – and continue to do so – by intentionally designing the Temu app, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and

retain the Plaintiffs' and the Subclass's private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information.

244. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendants' intrusion is heightened by Defendants' making the Plaintiffs' and the Subclass's private and personally identifiable data and content available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The intentionality of Defendants' conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendants' conduct targeted the Plaintiffs' and the Subclass's devices, which the United States Supreme Court has characterized as almost a feature of human anatomy, and which contain the Plaintiffs' and the Subclass's private and personally identifiable data and content.

245. The Plaintiffs and the Subclass were harmed by, and continue to suffer harm as a result of, the intrusion as detailed throughout this Complaint.

246. Defendants' conduct was a substantial factor in causing the harm suffered by the Plaintiffs and the Subclass.

247. The Plaintiffs and the Subclass seek nominal and punitive damages as a result of Defendants' actions. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were calculated to injure the Plaintiffs and the Subclass, and were made in

conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

248. The Plaintiffs and the Subclass seek injunctive relief to rectify Defendants' actions, including but not limited to requiring Defendants (a) to stop taking more private and personally identifiable data and content from the Plaintiffs' and the Subclass's devices and computers accounts than is reasonably necessary to operate the Temu app; (b) to make clear disclosures of the Plaintiffs' and the Subclass's private and personally identifiable data and content that is reasonably necessary to operate the Temu app; (c) to obtain the Plaintiffs' and the Subclass's consent to the taking of such private and personally identifiable data and content; (d) to stop providing access to the Plaintiffs' and the Subclass's private and personally identifiable data and content to individuals in China or transferring such data to servers or companies whose data is accessible from within China; and (e) to recall and destroy the Plaintiffs' and the Subclass's private and personally identifiable data and content already taken in contravention of the Plaintiffs' and the Subclass's privacy rights.

249. Plaintiffs and the Subclass seek restitution and disgorgement for Defendants' intrusion upon seclusion. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

TENTH COUNT:

**VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, BUS. & PROF. C. §§ 17200 *ET SEQ.*
(On Behalf Of the California Plaintiffs and California Subclass)**

250. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

251. The Unfair Competition Law, California Business & Professions Code §§ 17200, *et seq.* (the “UCL”), prohibits any “unlawful,” “unfair,” or “fraudulent” business act or practice, which can include false or misleading advertising.

252. Defendants violated, and continue to violate, the “unlawful” prong of the UCL through violation of statutes, constitutional provisions, and common law, as alleged herein.

253. Defendants violated, and continue to violate, the “unfair” prong of the UCL because they accessed private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information – from the Plaintiffs’ and the Subclass’s devices and computers under circumstances in which the Plaintiffs and the Subclass would have no reason to know that such data and content was being taken.

254. Plaintiffs and the Subclass had no reason to know because (i) there was no disclosure, or no effective disclosure, of Defendants’ collection and transfer of the Plaintiffs’ and the Subclass’s biometric identifiers and information, and private data and information; (ii) there was no disclosure that Defendants had embedded source code within the Temu app that makes Plaintiffs’ and the Subclass’s private and personally identifiable data and content accessible to third-party companies and individuals based in China where such companies and individuals are subject to Chinese law requiring the sharing of such data and content with the Chinese

government; and (iii) there was no effective disclosure of the wide range of private and personally identifiable data and content that Defendants took from the Plaintiffs' and the Subclass's devices. Defendants violated, and continue to violate, the "fraudulent" prong of the UCL because (i) Defendants made it appear that the Plaintiffs' private and personally identifiable data and content would not be collected and transferred unless the Plaintiffs and the Subclass chose to do so, but in fact Defendants collected and transferred such data and content without notice or consent; (ii) Defendants made it appear that the Plaintiffs' and the Subclass's private and personally identifiable data and content would not be provided to individuals or companies that are subject to Chinese law requiring the sharing of such data and content with the Chinese government; and (iii) Defendants have intentionally refrained from disclosing the uses to which the Plaintiffs' and the Subclass's private and personally identifiable data and content has been put, while simultaneously providing misleading reassurances about Defendants' data collection and use practices. The Plaintiffs and the Subclass were misled by Defendants' concealment, and had no reason to believe that Defendants had taken the private and personally identifiable data and content that they had taken or used it in the manner they did.

255. In addition, Defendants fail to adequately disclose that users' data will be accessible to individuals in China, and ultimately accessible by the Chinese communist government. To the contrary, Defendants assured Plaintiffs and the Subclass of the privacy of their data, while under Chinese law the Chinese government has an absolute right to access users' data.

256. Defendants' conduct is particularly egregious because these violations extend to minor users whom Defendants acknowledge should not be using the platform. Indeed, through their promotion through various influencers and other means, Defendants have encouraged minor

use. Moreover, they have failed to incorporate appropriate age verification and other measures in the Temu app necessary to prevent underage use and have incorporated features in the design of the Temu app that actually facilitate underage use.

257. In addition, Defendants have utilized a variety of deceptive, unfair and manipulative means to increase usage of the Temu app and, in turn, the collection of user data.

258. Plaintiffs and the Subclass have been harmed and have suffered economic injury as a result of Defendants' UCL violations. First, Plaintiffs and the Subclass have suffered harm in the form of diminution of the value of their private and personally identifiable data and content. Second, they have suffered harm to their devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed. Third, they have incurred additional data usage and electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming from Defendants' covert theft of their private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information.

259. Defendants, as a result of their conduct, have been able to reap unjust profits and revenues in violation of the UCL. This includes Defendants' profits and revenues from their targeted advertising, revenues from the sale of goods on the Temu site, and the increased consumer demand for and use of Defendants' products. Plaintiffs and the Subclass seek restitution and disgorgement of these unjust profits and revenues.

260. Unless restrained and enjoined, Defendants will continue to misrepresent their private and personally identifiable data and content collection and use practices, and will not recall

and destroy Plaintiffs' and the Subclass's wrongfully collected private and personally identifiable data and content. Accordingly, injunctive relief is appropriate.

ELEVENTH COUNT:

**VIOLATION OF THE CALIFORNIA FALSE ADVERTISING LAW, BUS. & PROF. C. §§ 17500 *ET SEQ.*
(On Behalf Of the California Plaintiffs and California Subclass)**

261. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

262. California's False Advertising Law (the "FAL") – Cal. Bus. & Prof. Code §§ 17500, *et seq.* – prohibits "any statement" that is "untrue or misleading" and made "with the intent directly or indirectly to dispose of" property or services.

263. Defendants' advertising is, and at all relevant times was, highly misleading. Defendants do not disclose at all, or do not meaningfully disclose, the private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and private data and information – that they have collected and transferred from the Plaintiffs' and the Subclass's devices and computers. Nor do Defendants disclose that the Plaintiffs' and the Subclass's private and personally identifiable data and content have been made available to foreign government entities.

264. Reasonable consumers, like the Plaintiffs and the Subclass, are – and at all relevant times were – likely to be misled by Defendants' misrepresentations. Reasonable consumers lack the means to verify Defendants' representations concerning their data and content collection and use practices, or to understand the fact or significance of Defendants' data and content collection and use practices.

265. Plaintiffs and the Subclass have been harmed and have suffered economic injury as a result of Defendants' misrepresentations. First, they have suffered harm in the form of diminution of the value of their private and personally identifiable data and content. Second, they have suffered harm to their devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed. Third, they have incurred additional data usage and electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming from Defendants' accessing their private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and other private data and information.

266. Defendants, as a result of their misrepresentations, have been able to reap unjust profits and revenues. This includes Defendants' profits and revenues from their targeted advertising, revenue from the sale of goods on the Temu site, and increased consumer demand for and use of Defendants' other products and services. Plaintiffs and the Subclass seek restitution and disgorgement of these unjust profits and revenues.

267. Unless restrained and enjoined, Defendants will continue to misrepresent their private and personally identifiable data and content collection and use practices and will not recall and destroy Plaintiffs' and the Subclass's wrongfully collected private and personally identifiable data and content. Accordingly, injunctive relief is appropriate.

TWELFTH COUNT:

**VIOLATION OF THE VIRGINIA COMPUTER CRIMES ACT, VA. CODE § 18.2-152.1, *ET SEQ.*
(On Behalf Of the Virginia Plaintiffs and Virginia Subclass)**

268. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

269. The Virginia Computer Crimes Act, Va. Code § 18.2-152.1, *et seq.*, prohibits the actions taken by Defendants to steal private data and content from Plaintiffs and the Virginia Subclass. Defendants have committed multiple violations of the Virginia Computer Crimes Act.

270. For each of the actions described below, the Virginia Computer Crimes Act provides a private right of action as follows:

A. Any person whose property or person is injured by reason of a violation of any provision of this article or by any act of computer trespass set forth in subdivisions A1 through A8 of § 18.2-152.4 regardless of whether such act is committed with malicious intent may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, “damages” shall include loss of profits.

* * *

E. The provisions of this article shall not be construed to limit any person’s right to pursue any additional civil remedy otherwise allowed by law.

Va. Code § 152.12(A).

271. Virginia Code section 18.2-152.3 provides:

Computer fraud; penalty.

Any person who uses a computer or computer network, without authority and:

1. Obtains property or services by false pretenses;
2. Embezzles or commits larceny; or
3. Converts the property of another;

is guilty of the crime of computer fraud. Va. Code § 18.2-152.3.

272. Under the Virginia Computer Crimes Act, “property” is defined broadly to include “computer data, computer programs, computer software and all other personal property.” Va. Code § 18.2-152.2.

273. By collecting Plaintiffs’ and the Subclass’s private data and information without their consent, Defendants have obtained property by false pretenses and converted that property, as described in the Virginia Computer Crimes Act.

274. Virginia Code § 18.2-152.4 provides:

Computer trespass, penalty.

A. It shall be unlawful for any person . . . to:

* * *

6. Use a computer or computer network to make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by, or produced by a computer or computer network.

Va. § 18.2-152.4.

275. By collecting Plaintiffs’ and the Subclass’s private data and information without their consent, Defendants used a computer or computer network to make an unauthorized copy of computer data residing in a computer or computer network, as described in the Virginia Computer Crimes Act.

276. Virginia Code § 18.2-152.5 provides:

Computer invasion of privacy; penalties.

- A. A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3, relating to any other person. “Examination” under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.

Va. Code § 18.2-152.5(A).

277. In turn, Virginia Code § 18.2-186.3 defines “identifying information” to include, inter alia, name, date of birth, and “biometric data,” which includes the sorts of private data and information Defendants collected from Plaintiffs’ and the Subclass.

278. By collecting the private data and information of Plaintiffs’ and the Subclass without their consent, Defendants used a computer or computer network to intentionally examine “identifying information,” including “biometric data,” and reviewed such information “after the time at which the offender knows or should know that he is without authority to view the information displayed.”

279. Virginia Code § 18.2-152.5:1 provides:

Using a computer to gather identifying information; penalties.

- A. It is unlawful for any person, other than a law-enforcement officer, as defined in § 9.1-101, and acting in the performance of his official duties, to use a computer to obtain, access, or record, through the use of material artifice, trickery or deception, any identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3.

Va. Code § 18.2-152.5(A).

280. Virginia Code § 18.2-186.3 defines “identifying information” to include, inter alia, name, date of birth, and “biometric data.”

281. By collecting Plaintiffs’ and the Subclass’s private data and information without their consent, Defendants used a computer to obtain, access and record, through the use of material artifice, trickery or deception, identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs respectfully request relief against Defendants as set forth below:

A. Entry of an order certifying the proposed class and subclass pursuant to Federal Rule of Civil Procedure 23, appointing Plaintiffs as representatives of the class and subclasses, appointing Plaintiffs’ counsel as co-lead counsel for the class and subclasses, and directing that notice be given to members of the class and subclasses;

B. Entry of an order declaring that Defendants’ actions, as set forth in this Complaint, violate the law;

C. Entry of judgment in favor of each class and subclass member for damages suffered as a result of the conduct alleged herein, including compensatory, statutory, and punitive damages, restitution, and disgorgement, in an amount to be determined at trial;

D. Award Plaintiffs pre- and post-judgment interest;

E. Award Plaintiffs their costs of suit, including reasonable attorneys’ fees and expenses;

F. Entry of a permanent injunction, enjoining Defendants from continuing conduct determined to be unlawful; and

G. Grant such other and further legal and equitable relief as the court deems just and equitable.

IX. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated this 3 day of November, 2023

Respectfully submitted,

HAGENS BERMAN SOBOL SHAPIRO LLP

By /s/ Steve W. Berman

Steve W. Berman
1301 Second Avenue, Suite 2000
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
steve@hbsslaw.com

Jeannie Evans
HAGENS BERMAN SOBOL SHAPIRO LLP
455 N. Cityfront Plaza Dr., Suite 2410
Chicago, IL 60611
Telephone: (708) 628-4962
Facsimile: (708) 628-4952
jeannie@hbsslaw.com

Douglas G. Smith
AURELIUS LAW GROUP LLC
77 West Wacker Drive, Suite 4500
Chicago, IL 60601
Telephone: (312) 451-6708
dsmith@aureliuslawgroup.com

Attorneys for Plaintiffs and the Class and Subclasses